

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2003-234728

(P2003-234728A)

(43)公開日 平成15年8月22日(2003.8.22)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0		3 2 0 F 5 J 1 0 4
		H 0 4 L 9/00	6 0 1 B
H 0 4 L 9/32			6 0 1 A
			6 7 5 B

審査請求 未請求 請求項の数83 O L (全 45 頁) 最終頁に続く

(21)出願番号 特願2002-259514(P2002-259514)  
(22)出願日 平成14年9月5日(2002.9.5)  
(31)優先権主張番号 特願2001-298414(P2001-298414)  
(32)優先日 平成13年9月27日(2001.9.27)  
(33)優先権主張国 日本(J P)  
(31)優先権主張番号 特願2001-374856(P2001-374856)  
(32)優先日 平成13年12月7日(2001.12.7)  
(33)優先権主張国 日本(J P)

(71)出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72)発明者 大森 基司  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 館林 誠  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(74)代理人 100109210  
弁理士 新居 広守

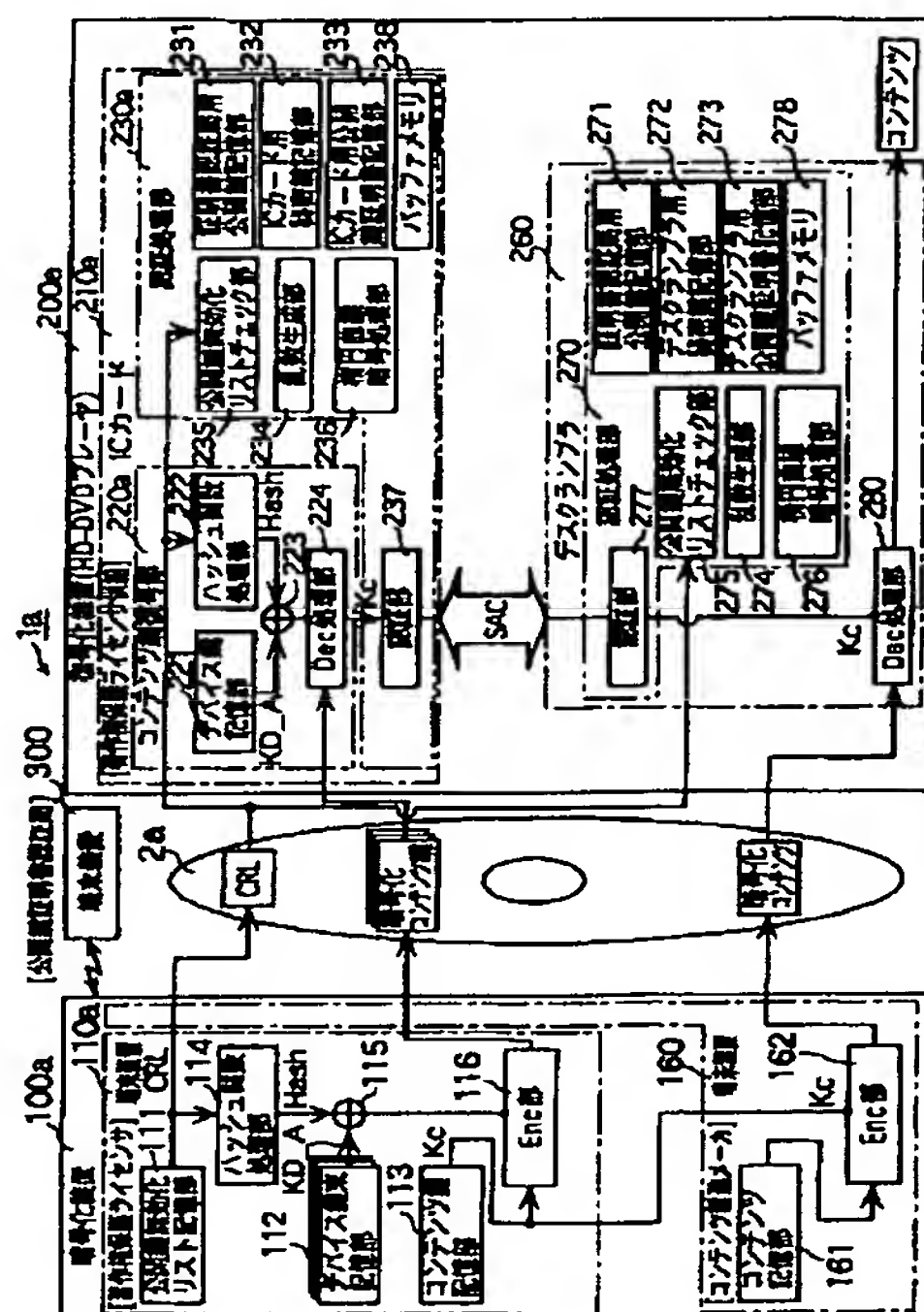
最終頁に続く

(54)【発明の名称】 暗号化装置、復号化装置、秘密鍵生成装置、著作権保護システムおよび暗号通信装置

(57)【要約】

【課題】 公開鍵証明書無効化リストの差し替え攻撃に対して防御することができ、安全にデジタル著作物を転送する暗号化装置を提供する。

【解決手段】 公開鍵証明書無効化リストを記憶する公開鍵無効化リスト記憶部111と、復号化装置200aで用いられるICカード210aごとに固有のデバイス鍵KD\_Aを記憶するデバイス鍵束記憶部112と、コンテンツを暗号化するための秘密鍵であるコンテンツ鍵Kcを記憶するコンテンツ鍵記憶部113と、ハッシュ関数にしたがって公開鍵無効化リスト記憶部111に記憶された公開鍵証明書無効化リストのハッシュ値を算出するハッシュ関数処理部114と、そのハッシュ値とデバイス鍵KD\_Aとの排他的論理和をとるE x - O R部115と、コンテンツ鍵KcをE x - O R部115の出力値で暗号化するE n c部116とを備える。





## 【特許請求の範囲】

【請求項1】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、  
 デジタル著作物を記憶するデジタル著作物記憶手段と、  
 デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、  
 暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
 無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、  
 前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記変形手段により変形された第2秘密鍵で暗号化する第1暗号化手段と、  
 前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化する第2暗号化手段と、  
 前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項2】 前記暗号化装置は、さらに、  
 前記復号化装置において復号化された第1秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項1記載の暗号化装置。

【請求項3】 前記確認データ出力手段は、所定の固定パターンのデータを前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項2記載の暗号化装置。

【請求項4】 前記確認データ出力手段は、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を当該第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項2記載の暗号化装置。

【請求項5】 前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、  
 前記変形手段は、前記第2秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第2秘密鍵を変形させることを特徴とする請求項1記載の暗号化装置。

【請求項6】 デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、  
 デジタル著作物を記憶するデジタル著作物記憶手段と、  
 デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、  
 暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、

10 無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、

前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で暗号化する第1暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

20 前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第1秘密鍵で暗号化する第2暗号化手段と、

前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

30 【請求項7】 前記暗号化装置は、さらに、  
 前記復号化装置において復号化された第1秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項6記載の暗号化装置。

40 【請求項8】 前記確認データ出力手段は、所定の固定パターンのデータを前記変形手段で変形された第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項7記載の暗号化装置。

【請求項9】 前記確認データ出力手段は、前記変形手段で変形された第1秘密鍵を当該第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項7記載の暗号化装置。

50 【請求項10】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、  
 デジタル著作物を記憶するデジタル著作物記憶手段と、  
 デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、



暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第1秘密鍵を記憶する第1秘密鍵記憶手段と、  
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
前記媒体識別情報記憶手段に記憶された媒体識別情報と前記変形手段で変形された第1秘密鍵とを一方向性関数に入力して変換する関数変換手段と、  
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第2暗号化手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項11】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、  
デジタル著作物を記憶するデジタル著作物記憶手段と、  
デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、  
暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第1秘密鍵を記憶する第1秘密鍵記憶手段と、  
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、  
前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第1秘密鍵記憶手段に記憶された第1秘密鍵とを一方向性関数に入力して変換する関数変換手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された属性値で暗号化する第1暗号化手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第1暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

- 【請求項12】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、  
デジタル著作物を記憶するデジタル著作物記憶手段と、  
デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、  
暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
前記第1秘密鍵の暗号化に用いられる第3秘密鍵を記憶する第3秘密鍵記憶手段と、  
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
前記第3秘密鍵記憶手段に記憶された第3秘密鍵を前記変形手段により変形された第2秘密鍵で暗号化する第1暗号化手段と、  
前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記第3秘密鍵記憶手段に記憶された第3秘密鍵で暗号化する第2暗号化手段と、  
前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化する第3暗号化手段と、  
前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第3秘密鍵、前記第2暗号化手段により暗号化された第1秘密鍵および前記第3暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。
- 【請求項13】 前記暗号化装置は、さらに、  
前記復号化装置において復号化された第3秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項12記載の暗号化装置。
- 【請求項14】 前記確認データ出力手段は、所定の固定パターンのデータを前記第3秘密鍵記憶手段に記憶された第3秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項13記載の暗号化装置。
- 【請求項15】 前記確認データ出力手段は、前記第3秘密鍵記憶手段に記憶された第3秘密鍵を当該第3秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項13記載の暗号化装置。



【請求項 16】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、前記第 1 秘密鍵の暗号化に用いられる第 3 秘密鍵を記憶する第 3 秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第 3 秘密鍵記憶手段に記憶された第 3 秘密鍵を前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で暗号化する第 1 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 3 秘密鍵記憶手段に記憶された第 3 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記変形手段で変形された属性値で暗号化する第 2 暗号化手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵で暗号化する第 3 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第 1 暗号化手段により暗号化された第 3 秘密鍵、前記第 2 暗号化手段により暗号化された第 1 秘密鍵および前記第 3 暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項 17】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、前記第 1 秘密鍵の暗号化に用いられる第 3 秘密鍵を記憶する第 3 秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第 3 秘密鍵記憶手段に記憶された第 3 秘密鍵を前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で暗号化する第 1 暗号化手段と、

前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記第 1 暗号化手段で暗号化された第 3 秘密鍵で暗号化する第 2 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

10 前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された第 1 秘密鍵で暗号化する第 3 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第 1 暗号化手段により暗号化された第 3 秘密鍵、前記第 2 暗号化手段により暗号化された第 1 秘密鍵および前記第 3 暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項 18】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、前記媒体識別情報の暗号化に用いられる第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を前記変形手段により変形された第 1 秘密鍵で暗号化する第 1 暗号化手段と、前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵とを一方方向性関数に入力して変換する関数変換手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第 2 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第 1 暗号化手段により暗号化された第 2 秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第 3 暗号化手段により暗号化された



デジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項 19】 前記暗号化装置は、さらに、前記復号化装置において復号化された第 2 秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えることを特徴とする請求項 18 記載の暗号化装置。

【請求項 20】 前記確認データ出力手段は、所定の固定パターンのデータを前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項 19 記載の暗号化装置。

【請求項 21】 前記確認データ出力手段は、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を当該第 2 秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力することを特徴とする請求項 19 記載の暗号化装置。

【請求項 22】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、前記媒体識別情報の暗号化に用いられる第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵で暗号化する第 1 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記媒体識別情報記憶手段に記憶された媒体識別情報と前記変形手段で変形された第 2 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記関数変換手段で得られた関数値で暗号化する第 2 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第 1 暗号化手段により暗号化された第 2 秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第 3 暗号化手段により暗号化された

デジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項 23】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる媒体識別情報を記憶する媒体識別情報記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、前記媒体識別情報の暗号化に用いられる第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵で暗号化する第 1 暗号化手段と、前記媒体識別情報記憶手段に記憶された媒体識別情報と前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段で変形された関数値で暗号化する第 2 暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第 1 暗号化手段により暗号化された第 2 秘密鍵、前記媒体識別情報記憶手段に記憶された媒体識別情報および前記第 2 暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする暗号化装置。

【請求項 24】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、暗号化されたデジタル著作物、その暗号化に用いられた第 1 秘密鍵を暗号化した暗号化第 1 秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該復号化装置に固有の第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変



形手段と、

前記取得手段により取得された暗号化第 1 秘密鍵を前記変形手段により変形された第 2 秘密鍵で復号化する第 1 復号化手段と、

前記取得手段により取得された暗号化デジタル著作物を前記第 1 復号化手段により復号化された第 1 秘密鍵で復号化する第 2 復号化手段とを備えることを特徴とする復号化装置。

【請求項 25】 前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、前記変形手段は、前記第 2 秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第 2 秘密鍵を変形させることを特徴とする請求項 24 記載の復号化装置。

【請求項 26】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第 1 秘密鍵を暗号化した暗号化第 1 秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、

前記取得手段により取得された暗号化第 1 秘密鍵を前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で復号化する第 1 復号化手段と、

前記取得手段に取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第 1 復号化手段により復号化された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された第 1 秘密鍵で復号化する第 2 復号化手段とを備えることを特徴とする復号化装置。

【請求項 27】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変

形手段と、

前記取得手段により取得された媒体識別情報と前記変形手段により変形された第 1 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第 1 復号化手段とを備えることを特徴とする復号化装置。

【請求項 28】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、

前記取得手段により取得された媒体識別情報と前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された属性値で復号化する第 1 復号化手段とを備えることを特徴とする復号化装置。

【請求項 29】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第 1 秘密鍵を暗号化した暗号化第 1 秘密鍵、前記第 1 秘密鍵の暗号化に用いられた第 2 秘密鍵を暗号化した暗号化第 2 秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第 3 秘密鍵を記憶する第 3 秘密鍵記憶手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第 3 秘密鍵記憶手段に記憶された第 3 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第 2 秘密鍵を前記変形手段により変形された第 3 秘密鍵で復号化する第 1 復号化手段と、

前記取得手段により取得された暗号化第 1 秘密鍵を前記第 1 復号化手段により復号化された第 2 秘密鍵で復号化する第 2 復号化手段と、



前記取得手段により取得された暗号化デジタル著作物を前記第2復号化手段により復号化された第1秘密鍵で復号化する第3復号化手段とを備えることを特徴とする復号化装置。

【請求項30】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵、前記第1秘密鍵の暗号化に用いられた第2秘密鍵を暗号化した暗号化第2秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第3秘密鍵を記憶する第3秘密鍵記憶手段と、

前記取得手段により取得された暗号化第2秘密鍵を前記第3秘密鍵記憶手段に記憶された第3秘密鍵で復号化する第1復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第1復号化手段で復号された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第1秘密鍵を前記変形手段により変形された第2秘密鍵で復号化する第2復号化手段と、

前記取得手段により取得された暗号化デジタル著作物を前記第2復号化手段により復号化された第1秘密鍵で復号化する第3復号化手段とを備えることを特徴とする復号化装置。

【請求項31】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵、前記第1秘密鍵の暗号化に用いられた第2秘密鍵を暗号化した暗号化第2秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第3秘密鍵を記憶する第3秘密鍵記憶手段と、

前記取得手段により取得された暗号化第2秘密鍵を前記第1秘密鍵記憶手段に記憶された第3秘密鍵で復号化する第1復号化手段と、

前記取得手段により取得された暗号化第1秘密鍵を前記第1復号化手段により復号化された第2秘密鍵で復号化する第2復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値

算出手段と、

前記第2復号化手段により復号化された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化デジタル著作物を前記変形手段により変形された第1秘密鍵で復号化する第3復号化手段とを備えることを特徴とする復号化装置。

【請求項32】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、

前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第1秘密鍵を前記変形手段により変形された第2秘密鍵で復号化する第1復号化手段と、

前記取得手段により取得された媒体識別情報と前記第1復号化手段により復号化された第1秘密鍵とを一方向性関数に入力して変換する関数変換手段と、

前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第2復号化手段とを備えることを特徴とする復号化装置。

【請求項33】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、

暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

当該復号化装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、

前記取得手段により取得された暗号化第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で復号化する第1復号化手段と、

取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値



算出手段と、  
 前記第1復号化手段で復号化された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記取得手段により取得された媒体識別情報と前記変形手段で変形された属性値とを一方向性関数に入力して変換する関数変換手段と、  
 前記取得手段により取得された暗号化デジタル著作物を前記関数変換手段で得られた関数値で復号化する第2復号化手段とを備えることを特徴とする復号化装置。  
 【請求項34】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置であって、  
 暗号化されたデジタル著作物、その暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、  
 当該復号化装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
 前記取得手段により取得された暗号化第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で復号化する第1復号化手段と、  
 前記取得手段により取得された媒体識別情報と前記第1復号化手段で復号された第1秘密鍵とを一方向性関数に入力して変換する関数変換手段と、  
 取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記取得手段により取得された暗号化デジタル著作物を前記変形手段で変形された関数値で復号化する第2復号化手段とを備えることを特徴とする復号化装置。  
 【請求項35】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、  
 デジタル著作物の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、  
 当該秘密鍵生成装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
 取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、

前記取得手段により取得された暗号化第1秘密鍵を前記変形手段により変形された第2秘密鍵で復号化する第1復号化手段と、  
 前記第1復号化手段により復号化された第1秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。  
 【請求項36】 前記秘密鍵生成装置は、さらに、  
 前記第1復号化手段により復号化された第1秘密鍵が前記デジタル著作物の暗号化に用いられた正しい第1秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項35記載の秘密鍵生成装置。  
 【請求項37】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 取得された確認データを前記第1復号化手段により復号化された第1秘密鍵で復号化する確認データ復号化部と、  
 前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項36記載の秘密鍵生成装置。  
 【請求項38】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 前記第1復号化手段により復号化された第1秘密鍵を当該第1秘密鍵で暗号化する第1秘密鍵暗号化部と、  
 前記第1秘密鍵暗号化部により暗号化された第1秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項36記載の秘密鍵生成装置。  
 【請求項39】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 前記確認データ取得部により取得された確認データを前記第1復号化手段により復号化された第1秘密鍵で復号化する確認データ復号化部と、  
 前記確認データ復号化部により復号化された値と前記第1復号化手段により復号化された第1秘密鍵とが一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項36記載の秘密鍵生成装置。  
 【請求項40】 前記属性値算出手段は、前記公開鍵無効化リストのハッシュ値を前記属性値として算出し、  
 前記変形手段は、前記第2秘密鍵と前記ハッシュ値との排他的論理和をとることによって、前記第2秘密鍵を変形させることを特徴とする請求項35記載の秘密鍵生成装置。



【請求項 4 1】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた第 1 秘密鍵を暗号化した暗号化第 1 秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該復号化装置に固有の第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、前記取得手段により取得された暗号化第 1 秘密鍵を前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で復号化する第 1 復号化手段と、前記取得手段に取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 1 復号化手段により復号化された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記変形手段で変形された第 1 秘密鍵を前記デジタル著作物の復号化のための秘密鍵として出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項 4 2】 前記秘密鍵生成装置は、さらに、前記変形手段により変形された第 1 秘密鍵が前記デジタル著作物の暗号化に用いられた正しい第 1 秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項 4 1 記載の秘密鍵生成装置。

【請求項 4 3】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、取得された確認データを前記変形手段で変形された第 1 秘密鍵で復号化する確認データ復号化部と、前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第 1 秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項 4 2 記載の秘密鍵生成装置。

【請求項 4 4】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、前記変形手段により変形された第 1 秘密鍵を当該第 1 秘密鍵で暗号化する第 1 秘密鍵暗号化部と、前記第 1 秘密鍵暗号化部により暗号化された第 1 秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第 1 秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項 4 2 記載の秘密鍵生成装置。

【請求項 4 5】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、前記確認データ取得部により取得された確認データを前

記変形手段により変形された第 1 秘密鍵で復号化する確認データ復号化部と、前記確認データ復号化部により復号化された値と前記変形手段により変形された第 1 秘密鍵とが一致するか否かを判定し、一致する場合に、前記第 1 秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項 4 2 記載の秘密鍵生成装置。

【請求項 4 6】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該復号化装置に固有の第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記取得手段により取得された媒体識別情報と前記変形手段により変形された第 1 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項 4 7】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた媒体識別情報および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該復号化装置に固有の第 1 秘密鍵を記憶する第 1 秘密鍵記憶手段と、前記取得手段により取得された媒体識別情報と前記第 1 秘密鍵記憶手段に記憶された第 1 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記変形手段で変形された属性値を前記デジタル著作物の復号化のための秘密鍵として出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項 4 8】 暗号化されたデジタル著作物を復号化



する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵、前記第1秘密鍵の暗号化に用いられた第2秘密鍵を暗号化した暗号化第2秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該秘密鍵生成装置に固有の第3秘密鍵を記憶する第3秘密鍵記憶手段と、取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第3秘密鍵記憶手段に記憶された第3秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記取得手段により取得された暗号化第2秘密鍵を前記変形手段により変形された第3秘密鍵で復号化する第1復号化手段と、前記取得手段により取得された暗号化第1秘密鍵を前記第1復号化手段により復号化された第2秘密鍵で復号化する第2復号化手段と、前記第2復号化手段により復号化された第1秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項49】 前記秘密鍵生成装置は、さらに、前記第1復号化手段により復号化された第2秘密鍵が前記第1秘密鍵の暗号化に用いられた正しい第2秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項48記載の秘密鍵生成装置。

【請求項50】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、取得された確認データを前記第1復号化手段により復号化された第2秘密鍵で復号化する確認データ復号化部と、前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第2秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項49記載の秘密鍵生成装置。

【請求項51】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、前記第1復号化手段により復号化された第2秘密鍵を当該第2秘密鍵で暗号化する第2秘密鍵暗号化部と、前記第2秘密鍵暗号化部により暗号化された第2秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第2秘

秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項49記載の秘密鍵生成装置。

【請求項52】 前記判定手段は、前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、前記確認データ取得部により取得された確認データを前記第1復号化手段により復号化された第2秘密鍵で復号化する確認データ復号化部と、前記確認データ復号化部により復号化された値と前記第1復号化手段により復号化された第2秘密鍵とが一致するか否かを判定し、一致する場合に、前記第2秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項49記載の秘密鍵生成装置。

【請求項53】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵、前記第1秘密鍵の暗号化に用いられた第2秘密鍵を暗号化した暗号化第2秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、当該復号化装置に固有の第3秘密鍵を記憶する第3秘密鍵記憶手段と、前記取得手段により取得された暗号化第2秘密鍵を前記第3秘密鍵記憶手段に記憶された第3秘密鍵で復号化する第1復号化手段と、取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第1復号化手段で復号された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記取得手段により取得された暗号化第1秘密鍵を前記変形手段により変形された第2秘密鍵で復号化する第2復号化手段と、前記第2復号化手段により復号化された第1秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項54】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、デジタル著作物の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵、前記第1秘密鍵の暗号化に用いられた第2秘密鍵を暗号化した暗号化第2秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、

前記取得手段により取得された暗号化第2秘密鍵を前記



第1秘密鍵記憶手段に記憶された第3秘密鍵で復号化する第1復号化手段と、  
 前記取得手段により取得された暗号化第1秘密鍵を前記第1復号化手段により復号化された第2秘密鍵で復号化する第2復号化手段と、  
 取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記第2復号化手段により復号化された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記第2復号化手段により復号化された第1秘密鍵を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項55】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、  
 デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、  
 当該秘密鍵生成装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
 取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記取得手段により取得された暗号化第1秘密鍵を前記変形手段により変形された第2秘密鍵で復号化する第1復号化手段と、  
 前記取得手段により取得された媒体識別情報と前記第1復号化手段により復号化された第1秘密鍵とを一方方向性関数に入力して変換する関数変換手段と、  
 前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項56】 前記秘密鍵生成装置は、さらに、  
 前記第1復号化手段により復号化された第1秘密鍵が前記媒体識別情報の暗号化に用いられた正しい第1秘密鍵である否かを判定する判定手段を備えることを特徴とする請求項55記載の秘密鍵生成装置。

【請求項57】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 取得された確認データを前記第1復号化手段により復号

化された第1秘密鍵で復号化する確認データ復号化部と、  
 前記確認データ復号化部による復号化によって得られたデータが所定の固定パターンに一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項56記載の秘密鍵生成装置。

【請求項58】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 前記第1復号化手段により復号化された第1秘密鍵を当該第1秘密鍵で暗号化する第1秘密鍵暗号化部と、  
 前記第1秘密鍵暗号化部により暗号化された第1秘密鍵が前記確認データ取得部により取得された確認データと一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項56記載の秘密鍵生成装置。

【請求項59】 前記判定手段は、  
 前記記録媒体又は伝送媒体から前記判定の基準となる確認データを取得する確認データ取得部と、  
 前記確認データ取得部により取得された確認データを前記第1復号化手段により復号化された第1秘密鍵で復号化する確認データ復号化部と、  
 前記確認データ復号化部により復号化された値と前記第1復号化手段により復号化された第1秘密鍵とが一致するか否かを判定し、一致する場合に、前記第1秘密鍵が正しいものであると判定する判定部とを有することを特徴とする請求項56記載の秘密鍵生成装置。

【請求項60】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、  
 デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第1秘密鍵を暗号化した暗号化第1秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、  
 当該復号化装置に固有の第2秘密鍵を記憶する第2秘密鍵記憶手段と、  
 前記取得手段により取得された暗号化第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で復号化する第1復号化手段と、  
 取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
 前記第1復号化手段で復号化された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
 前記取得手段により取得された媒体識別情報と前記変形手段で変形された属性値とを一方方向性関数に入力して変換する関数変換手段と、



前記関数変換手段で得られた関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項 6 1】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置であって、  
デジタル著作物の暗号化に用いられた媒体識別情報、前記媒体識別情報の暗号化に用いられた第 1 秘密鍵を暗号化した暗号化第 1 秘密鍵および無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得する取得手段と、  
当該復号化装置に固有の第 2 秘密鍵を記憶する第 2 秘密鍵記憶手段と、  
前記取得手段により取得された暗号化第 1 秘密鍵を前記第 2 秘密鍵記憶手段に記憶された第 2 秘密鍵で復号化する第 1 復号化手段と、  
前記取得手段により取得された媒体識別情報と前記第 1 復号化手段で復号された第 1 秘密鍵とを一方向性関数に入力して変換する関数変換手段と、  
取得された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、  
前記関数変換手段で得られた関数値を前記属性値算出手段により算出された属性値で変形させる変形手段と、  
前記変形手段で変形された関数値を前記デジタル著作物の復号化のための秘密鍵として前記復号化装置に出力する出力手段とを備えることを特徴とする秘密鍵生成装置。

【請求項 6 2】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、  
請求項 1 記載の暗号化装置と請求項 2 4 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 3】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、  
請求項 5 記載の暗号化装置と請求項 2 5 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 4】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、  
請求項 6 記載の暗号化装置と請求項 2 6 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 5】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 1 0 記載の暗号化装置と請求項 2 7 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 6】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 1 1 記載の暗号化装置と請求項 2 8 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

10 【請求項 6 7】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 1 2 記載の暗号化装置と請求項 2 9 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 8】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

20 請求項 1 6 記載の暗号化装置と請求項 3 0 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 6 9】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 1 7 記載の暗号化装置と請求項 3 1 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

30 【請求項 7 0】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 1 8 記載の暗号化装置と請求項 3 2 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 7 1】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 2 2 記載の暗号化装置と請求項 3 3 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

40 【請求項 7 2】 記録媒体又は伝送媒体を介してデジタル著作物を安全に伝送するための著作権保護システムであって、

請求項 2 3 記載の暗号化装置と請求項 3 4 記載の復号化装置とから構成されることを特徴とする著作権保護システム。

【請求項 7 3】 相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、  
無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、

50 新たな公開鍵無効化リストを取得する取得手段と、



取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、

前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする暗号通信装置。

【請求項 7 4】 相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、新たな公開鍵無効化リストを取得する取得手段と、取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする暗号通信装置。

【請求項 7 5】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、 $n$  ( $\geq 2$ ) 個の秘密鍵のうち、第 1 秘密鍵を用いてデジタル著作物を暗号化するとともに、第  $i$  ( $2 \leq i \leq n$ ) 秘密鍵を用いて第  $(i-1)$  秘密鍵を暗号化するという暗号化の連鎖を前記第 1 ～第  $(n-1)$  秘密鍵について繰り返し、暗号化された第 1 ～第  $(n-1)$  秘密鍵を前記媒体に出力する方法であって、前記第 1 ～第  $n$  秘密鍵の少なくとも 1 つを用いた暗号化においては、その暗号化に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておく第 1 ステップを含むことを特徴とする暗号化方法。

【請求項 7 6】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、 $n$  ( $\geq 1$ ) 個の秘密鍵のうち、第 1 秘密鍵を用いて媒体識別情報を一方向性関数で変換した後に、変換された媒体識別情報でデジタル著作物を暗号化するとともに、前記  $n$  が 2 以上の場合に、第  $i$  ( $2 \leq i \leq n$ ) 秘密鍵を用いて第  $(i-1)$  秘密鍵を暗号化するという暗号化の連鎖を前記第 1 ～第  $(n-1)$  秘密鍵について繰り返し、暗号化された第 1 ～第  $(n-1)$  秘密鍵を前記媒体に出力する方法であって、前記第 1 ～第  $n$  秘密鍵の少なくとも 1 つを用いた暗号化又は変換においては、(i) その暗号化又は変換に先立ち、無効化された公開鍵証明書を特定する情報の一覧で

ある公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくか、又は、(2) 前記変換によって得られた媒体識別情報を前記属性値で変形させておく第 2 ステップを含むことを特徴とする暗号化方法。

【請求項 7 7】 暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と  $n$  ( $\geq 2$ ) 個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記  $n$  個の暗号化秘密鍵のうちの第 1 暗号化秘密鍵を復号化し、得られた第 1 秘密鍵で第 2 暗号化秘密鍵を復号化するという復号化の連鎖を前記  $n$  個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第  $n$  秘密鍵でデジタル著作物を復号化する方法であって、

前記第 1 ～第  $n$  暗号化秘密鍵に対する復号化の少なくとも 1 つにおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておく第 3 ステップを含むことを特徴とする復号化方法。

【請求項 7 8】 暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と媒体識別情報と  $n$  ( $\geq 1$ ) 個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記  $n$  個の暗号化秘密鍵のうちの第 1 暗号化秘密鍵を復号化し、前記  $n$  が 2 以上の場合に、前記復号化で得られた第 1 秘密鍵で第 2 暗号化秘密鍵を復号化するという復号化の連鎖を前記  $n$  個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第  $n$  秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報でデジタル著作物を復号化する方法であって、

前記第 1 ～第  $n$  暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも 1 つにおいては、

(1) その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、(2) 前記変換によって得られた媒体識別情報を前記属性値で変形させておく第 4 ステップを含むことを特徴とする復号化方法。

【請求項 7 9】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置において、 $n$  ( $\geq 2$ ) 個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記  $n$  個の暗号化秘密鍵のうちの第 1 暗号化秘密鍵を復号化し、得られた第 1 秘密鍵で第 2 暗号化秘密鍵を復号化するという復号化の連鎖を前記  $n$  個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第  $n$  秘密鍵を前



記復号化装置に出力する方法であって、  
前記第1～第n暗号化秘密鍵に対する復号化の少なくとも1つにおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておく第5ステップを含むことを特徴とする秘密鍵生成方法。

【請求項80】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置において、媒体識別情報とn（ $\geq 1$ ）個の暗号化秘密鍵と無効化された公開鍵証明書とを特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記n個の暗号化秘密鍵のうちの第1暗号化秘密鍵を復号化し、前記nが2以上の場合に、前記復号化で得られた第1秘密鍵で第2暗号化秘密鍵を復号化するという復号化の連鎖を前記n個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第n秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報を前記復号化装置に出力する方法であって、

前記第1～第n暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも1つにおいては、

（1）その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、（2）前記変換によって得られた媒体識別情報を前記属性値で変形させておく第6ステップを含むことを特徴とする秘密鍵生成方法。

【請求項81】 デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置に用いられるプログラムであって、  
請求項75又は76記載の暗号化方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【請求項82】 記録媒体又は伝送媒体を介して、暗号化されたデジタル著作物を取得し、復号化する復号化装置に用いられるプログラムであって、  
請求項77又は78記載の復号化方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【請求項83】 暗号化されたデジタル著作物を復号化する復号化装置に対して、復号化のための秘密鍵を出力する秘密鍵生成装置に用いられるプログラムであって、  
請求項79又は80記載の秘密鍵生成方法におけるステップをコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、記録媒体又は伝送媒体を介してデジタル著作物を転送する際の著作権保護

を図る暗号化装置および復号化装置等に関し、特に、無効化された公開鍵証明書を特定する公開鍵証明書無効化リストの差し替え攻撃に対する防御技術に関する。

【0002】

【従来の技術】デジタル著作物を第1の機器から第2の機器に転送する際に、不正取得による著作権侵害を防止するために、転送に先立ち、第1の機器が第2の機器を認証する（あるいは、相互に認証する）ことが行われる。つまり、通信相手が確かに自分が意図している相手かどうかを確認することが行われる。

【0003】例えば、公開鍵暗号を用いた例として、第1の機器が第2の機器に乱数を送信し、続いて、第2の機器がその乱数に対して自分の秘密鍵で暗号化（電子署名など）して第1の機器に返信し、最後に、返信されてきた暗号文（あるいは、署名文）に対して、第1の機器が第2の機器の公開鍵を用いて検証するというものである。ところが、このような公開鍵暗号を用いた認証においては、公開鍵そのものが有効なものであることが前提となる。

【0004】そこで、最近では、認証局と呼ばれる機関あるいは企業から、各ユーザに対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）

「公開鍵証明書」が発行されるようになってきた。そして、発行された公開鍵証明書のうち、有効期限の過ぎたものや、不正を働いたユーザあるいは秘密鍵が盗まれたユーザの公開鍵証明書等については、それらが無効化させるために（無効化していることを他のユーザに知らせるために）、無効化した公開鍵証明書を特定する情報の一覧を示す公開鍵証明書無効化リスト（Certificate Revocation List；以下、「CRL」、「公開鍵無効化リスト」又は「無効化リスト」等とも記す。）が発行されている。

【0005】したがって、通信相手の公開鍵を用いてその通信相手を認証する際には、その通信相手から公開鍵証明書を入手し、入手した公開鍵証明書が公開鍵証明書無効化リストに登録されたもの（無効化されたもの）でないことを確認した上で、上述の認証処理を行うことで、不正な通信相手に貴重なデジタル著作物を渡してしまうことを回避することができる。

【0006】なお、公開鍵証明書だけを用いて鍵を検証しているものもあるが（例えば、特許文献1参照。）、上記したように、有効期限の過ぎたものや、不正を働いたユーザあるいは秘密鍵が盗まれたユーザの公開鍵証明書等については、対処できない。

【0007】

【特許文献1】特許第3199119号公報（第2頁）

【0008】

【発明が解決しようとする課題】しかしながら、あらゆる機器が、正規の公開鍵証明書無効化リストを入手して通信相手の公開鍵証明書の有効性をチェックできるとは



限らず、そのために、その弱点を利用した不正行為が行われる可能性がある。

【0009】例えば、映画等のデジタル著作物が記録されたDVD (Digital Video/Versatile Disc) を再生するDVDドライブ装置等の機器が、DVDを介して正規の公開鍵証明書無効化リストを取得し (DVDに記録された最新の公開鍵証明書無効化リストを読み出し)、その公開鍵証明書無効化リストを用いて、相手機器 (内蔵の再生処理回路や再生用ソフトウェアが稼動するコンピュータ等) を認証する方法を採用した場合には、公開鍵証明書無効化リストを読み出す過程において、例えば、古い公開鍵証明書無効化リストに差し替えられてしまう可能性がある。そのために、正規の (例えば、最新の) 公開鍵証明書無効化リストであれば無効化された公開鍵証明書として登録されているにも拘わらず、すり替えられた古い公開鍵証明書無効化リストには未だ登録されていない無効な公開鍵を用いて、不正にデジタル著作物が取得されてしまうという攻撃を受け得る。

【0010】また、既に公開鍵証明書無効化リストを保持している機器が新たな公開鍵証明書無効化リストを入手した際に、いずれの公開鍵証明書無効化リストがより最新であるか、すなわち、保存しておくべき公開鍵証明書無効化リストはいずれであるかを的確に判断する必要もある。

【0011】そこで、本発明は、このような状況に鑑みてなされたものであり、公開鍵証明書無効化リストの差し替えという攻撃に対して防御することができ、安全にデジタル著作物を転送することを可能にする暗号化装置、復号化装置、秘密鍵生成装置、著作権保護システムおよび暗号通信装置を提供することを第1の目的とする。また、本発明の第2の目的は、公開鍵証明書無効化リストを用いて暗号通信をする装置において、新たな公開鍵証明書無効化リストを入手したときに、より最新のものを的確に特定し、古いものに代えて、より最新の公開鍵証明書無効化リストを保持することを可能にすることである。

【0012】

【課題を解決するための手段】上記第1の目的を達成するために、本発明に係る暗号化装置は、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第

2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記変形手段により変形された第2秘密鍵で暗号化する第1暗号化手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化する第2暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【0013】ここで、前記暗号化装置は、さらに、前記復号化装置において復号化された第1秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えてもよい。例えば、前記確認データ出力手段は、所定の固定パターンのデータを前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力したり、前記確認データ出力手段は、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を当該第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力してもよい。

【0014】また、本発明に係る暗号化装置は、デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で暗号化する第1暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第1秘密鍵で暗号化する第2暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【0015】また、上記第2の目的を達成するために、



本発明に係る暗号通信装置は、相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、無効化された公開鍵証明書を持定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、新たな公開鍵無効化リストを取得する取得手段と、取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする。同様に、上記格納手段に代えて、取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段とすることもできる。

【0016】なお、本発明は、上記暗号化装置に対応する復号化装置あるいは秘密鍵生成装置として実現したり、それら暗号化装置および復号化装置からなる著作権保護システムとして実現したり、それら暗号化装置、復号化装置および暗号通信装置を構成する特徴的な手段をステップとする暗号化方法、復号化方法および暗号通信方法として実現したり、それらステップをパーソナルコンピュータ等に実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをDVD等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは言うまでもない。

【0017】

【発明の実施の形態】以下、本発明の実施の形態に係る著作権保護システムについて、図面を用いて詳細に説明する。

【0018】（実施の形態1）図1は、本実施の形態1に係る記録メディア用著作権保護システムの全体構成を示す機能ブロック図である。記録メディア用著作権保護システム1aは、記録メディアとしてのDVD2aに暗号化されたコンテンツ等を記録したり、DVD2aから暗号化されたコンテンツ等を読み出してコンテンツを復号化したりするものであり、DVD2aに暗号化されたコンテンツ等を記録する暗号化装置100aと、DVD2aから暗号化されたコンテンツ等を読み出してコンテンツを復号化する復号化装置200aと、公開鍵証明書無効化リストCRL等を発行する公開鍵証明書認証局（Certificate Authority）CAが使用する端末装置300などから構成される。

【0019】暗号化装置100aは、大きく分けて、2台の端末装置、すなわち、著作権保護ライセンスが使用

する端末装置110aと、コンテンツ製造メーカーが使用する端末装置160とから構成される。

【0020】復号化装置200aは、例えば画質レベルHD（1125i/750p）でのコンテンツ再生に対応したHD-DVDプレーヤ等であって、著作権保護ライセンスが供給するICカード210aと、このプレーヤの製造メーカーのデスクランブラ260と、DVD2aから暗号化されたコンテンツ等を読み出すDVD-ROMドライブ（不図示）等とからなる。

10 【0021】著作権保護ライセンスが使用する端末装置110aは、復号化装置200aにおいて著作権保護を図るための情報、すなわち公開鍵証明書無効化リストCRL、コンテンツを復号化するためのコンテンツ鍵、このコンテンツ鍵を暗号化した暗号化コンテンツ鍵の束を端末装置160に提供するコンピュータ装置であり、その機能として、公開鍵無効化リスト記憶部111と、デバイス鍵束記憶部112と、コンテンツ鍵記憶部113と、ハッシュ関数処理部114と、Ex-OR部115と、Enc部116等とを備える。

20 【0022】公開鍵無効化リスト記憶部111は、インターネット等の通信網を介して端末装置300に定期的にアクセスし、公開鍵証明書認証局CAが提供する最新の公開鍵証明書無効化リストCRLを定期的に更新記憶する。この公開鍵証明書無効化リストCRLは、図2に示されるように、ファイルヘッダと、「全般」のフィールドと、「無効リスト」のフィールド等とからなる。ファイルヘッダには、ファイルの「名前」○△□△.crl、ファイルの「サイズ」79KB、ファイルの「種類」証明書無効リスト、ファイルの「更新日」2001/09/07/12:34のレコードを含む。また、

30 「全般」フィールドには、「バージョン」V1、「発行者」○△□△、「有効開始日」2001年9月6日、「次の更新予定日」2001年9月16日、「署名アルゴリズム」md5RASのレコードを含む。また、「無効リスト」のフィールドには、無効となった証明書のシリアル番号と、その無効日とのレコードがテキスト形式で記載されている。この公開鍵証明書無効化リストCRLは、時が経つにつれて無効となった証明書の数が単調の増え続けるため、最新版であるほど、無効となった証明書のシリアル番号のエントリー数（リスト登録台数）が単調増加し、ファイルの「サイズ」が単調的に大きくなる性質を有している。

40 【0023】デバイス鍵束記憶部112は、著作権保護ライセンスが供給するICカード210aごとに固有のデバイス鍵KD\_A（例えば、128bit）を束にして予め記憶する。

50 【0024】コンテンツ鍵記憶部113は、映画や音楽等の所定のコンテンツを暗号化するための秘密鍵であるコンテンツ鍵Kc（例えば、128bit）を記憶する。



【0025】ハッシュ関数処理部114は、ハッシュ関数にしたがって、公開鍵無効化リスト記憶部111に記憶された可変長のデータである公開鍵証明書無効化リストCRLを圧縮して固定長（例えば、128bit）のデータ（ハッシュ値Hash）に変換する処理部であり、例えば、SHA-1（Secure Hash Algorithm-1）やMD5などにしたがって変換する。

【0026】Ex-OR部115は、ハッシュ関数処理部114により算出されたハッシュ値Hashと、デバイス鍵束記憶部112に記憶された各デバイス鍵KD\_Aとの排他的論理和をとる（各デバイス鍵KD\_Aをハッシュ値Hashで変形させる）。

【0027】Enc部116は、コンテンツ鍵記憶部113に記憶されたコンテンツ鍵KcをEx-OR部115の出力、すなわちハッシュ値Hashと各デバイス鍵KD\_Aとの排他的論理和値で暗号化し、暗号化コンテンツ鍵の束を生成する。

【0028】なお、この端末装置110aのハッシュ関数処理部114およびEx-OR部115は、公開鍵無効化リスト記憶部111に記憶された公開鍵証明書無効化リストCRLに依存させてデバイス鍵KD\_Aを変形させているが、これは、変形されたデバイス鍵KD\_Aでコンテンツ鍵Kcを暗号化させることで、Enc部116から出力される暗号化コンテンツ鍵と公開鍵証明書無効化リストCRLとを関連付けるためである。これによって、後述する復号化装置200aでの復号処理において、公開鍵証明書無効化リストCRLの差し替えという攻撃に対して防御することが可能となる。

【0029】コンテンツ製造メーカーが使用する端末装置160は、端末装置110aから渡された公開鍵証明書無効化リストCRLや、暗号化コンテンツ鍵の束をそのままDVD2aに記録したりする書き込み装置であり、その機能として、コンテンツ記憶部161と、Enc部162等とを備える。

【0030】コンテンツ記憶部161は、映画や音楽等の所定のコンテンツを予め記憶する。

【0031】Enc部162は、コンテンツ記憶部161に記憶されたコンテンツを、端末装置110aから渡されたコンテンツ鍵Kcで暗号化し、暗号化コンテンツを生成する。

【0032】このように2台の端末装置110a、160から構成された暗号化装置100aにおいては、DVD2aを製造する場合、端末装置110aは、公開鍵無効化リスト記憶部111から公開鍵無効化リストCRLを読み出して、読み出した公開鍵無効化リストCRLをハッシュ関数処理部114と、端末装置160とに渡す。ハッシュ関数処理部114は、公開鍵無効化リストCRLのハッシュ値Hashを計算し、計算したハッシュ値HashをEx-OR部115に渡す。Ex-OR部115は、デバイス鍵束記憶部112からデバイス鍵

KD\_A、…を1つずつ読み出し、読み出すごとにデバイス鍵KD\_A、…とハッシュ値Hashとの排他的論理和を順次計算し、各排他的論理和値をEnc部116に出力する。そして、端末装置110aは、コンテンツ鍵記憶部113からコンテンツ鍵Kcを読み出して、読み出したコンテンツ鍵KcをEnc部116と、端末装置160とに渡す。Enc部116は、渡されたコンテンツ鍵KcをEx-OR部115から出力された各排他的論理和値で暗号化する。すなわち、Enc部116は、デバイス鍵KD\_Aのそれぞれの値とハッシュ値Hashとの排他的論理和値を鍵として、コンテンツ鍵Kcを暗号化する。これにより、Enc部116は、暗号化したコンテンツ鍵を複数生成し、暗号化コンテンツ鍵を束にして端末装置160に渡す。

【0033】端末装置160は、端末装置110aから渡された公開鍵無効化リストCRLと、暗号化コンテンツ鍵の束とを、そのままDVD2aに書き込む。そして、Enc部162により生成された暗号化コンテンツをDVD2aに書き込む。このようにして製造されたDVD2aは、暗号化コンテンツと共に、暗号化コンテンツ鍵の束と、製造時点で最新の公開鍵無効化リストCRLとがバインドされた状態でユーザに販売される。

【0034】一方、このようなDVD2aを復号化する復号化装置200aのICカード210aは、コンピュータのプログラムを故意の変更から防ぐために使用されるモジュール（TRM: Tamper Resistance Module）で構成され、公開鍵証明書無効化リストCRLに載るような不正なデスクランブラ260を排除することにより著作権を保護するものであって、大きく分けて、DVD2aにバインドされた公開鍵証明書無効化リストCRLに基づいて暗号化コンテンツを復号するための鍵を取得するコンテンツ鍵復号部220aと、公開鍵無効化リストCRLにより通信相手（デスクランブラ260）がRevoke（無効化）されていないかどうかをチェックしつつ、デスクランブラ260との間の相互認証形式でSAC（Secure Authentication Channel: 認証付け安全な通信路）を設定するための認証処理部230aとを備える。

【0035】認証処理部230aは、証明書認証局用公開鍵記憶部231と、ICカード用秘密鍵記憶部232と、ICカード用（著作権保護ライセンス用）公開鍵証明書記憶部233と、乱数生成部234と、公開鍵無効化リストチェック部235と、楕円曲線暗号処理部236と、認証部237と、バッファメモリ238等とからなる。

【0036】証明書認証局用公開鍵記憶部231は、公開鍵証明書認証局CAの署名を解読するのに用いる認証局用公開鍵PK\_CAを予め記憶する。

【0037】ICカード用秘密鍵記憶部232は、著作権保護ライセンスから供給されたICカード210aが



自己の署名に用いるICカードに固有のICカード用秘密鍵SK\_\_Aを予め記憶する。

【0038】ICカード用公開鍵証明書記憶部233は、公開鍵PK\_\_AがICカード210aのものであることを公開鍵証明書認証局CAが証明する書類であるICカード用公開鍵証明書Cert\_\_Aを予め記憶する。このICカード用公開鍵証明書Cert\_\_Aは、図3に示されるように、ICカード210a（著作権保護ライセンス）のIDや、ICカード用秘密鍵SK\_\_Aに対するICカード用公開鍵PK\_\_A、ICカード用公開鍵PK\_\_Aに対する証明書認証局CAの署名、（証明書の）有効期限等から構成される。

【0039】乱数生成部234は、時変の値として乱数（例えば、128bit）を生成する。

【0040】公開鍵無効化リストチェック部235は、公開鍵無効化リストCRLに相手（デスクランブラ260）のIDが含まれているか否かをチェックする。

【0041】楕円曲線暗号処理部236は、SAC設定における認証等の際に、楕円曲線にしたがった暗号処理（例えば、256bitの処理単位）を実行する。

【0042】認証部237は、SACを介してデスクランブラ260と通信する通信インタフェースである。

【0043】バッファメモリ238は、乱数生成部234が生成した乱数や、楕円曲線暗号処理部236が生成した一時的なデータを保持する。

【0044】コンテンツ鍵復号部220は、デバイス鍵記憶部221と、ハッシュ関数処理部222と、E x-O R部223と、D e c処理部224とを備える。

【0045】デバイス鍵記憶部221は、ICカード210aに固有のデバイス鍵KD\_\_A（秘密鍵であり、例えば、AES128bitの鍵）を記憶する。

【0046】ハッシュ関数処理部222は、端末装置110aのハッシュ関数処理部114と同様に構成され、DVD2aにバインドされた公開鍵証明書無効化リストCRLのハッシュ値Hash（例えば、128bit）を算出する。

【0047】E x-O R部223は、デバイス鍵記憶部221に記憶されたデバイス鍵KD\_\_Aと、ハッシュ関数処理部222により算出されたハッシュ値Hashとの排他的論理和をとる（つまり、デバイス鍵KD\_\_Aをハッシュ値Hashで変形させる）。

【0048】D e c処理部224は、DVD2aにバインドされた暗号化コンテンツ鍵の束の中から予め定められた場所に記録されている自己用の暗号化コンテンツ鍵を、デバイス鍵KD\_\_Aとハッシュ値Hashとの排他的論理和値で復号化し、コンテンツ鍵Kcを生成する。

【0049】デスクランブラ260は、ICカード210aと同様、コンピュータプログラムの不正な改ざんを防ぐために使用されるモジュールで構成され、大きく分けて、公開鍵無効化リストCRLにより通信相手（IC

カード210a）がR e v o k eされていないかどうかをチェックしつつ、ICカード210aとの間の相互認証形式でSACを設定するための認証処理部270と、DVD2aから読み出した暗号化コンテンツを、ICカード210aから渡されたコンテンツ鍵Kcで復号し、コンテンツを取得するD e c処理部280とを備える。

【0050】認証処理部270は、証明書認証局用公開鍵記憶部271と、デスクランブラ用秘密鍵記憶部272と、デスクランブラ用（プレーヤメカ用）公開鍵証明書記憶部273と、乱数生成部274と、公開鍵無効化リストチェック部275と、楕円曲線暗号処理部276と、認証部277と、バッファメモリ278等とからなる。

【0051】証明書認証局用公開鍵記憶部271は、証明書認証局CAの証明書認証局用公開鍵PK\_\_CAを予め記憶する。

【0052】デスクランブラ用秘密鍵記憶部272は、このHD-DVDプレーヤ200のメカにより供給され、デスクランブラ260が自己の署名に用いるデスクランブラに固有のデスクランブラ用秘密鍵SK\_\_iを予め記憶する。

【0053】デスクランブラ用公開鍵証明書記憶部273は、公開鍵PK\_\_iがプレーヤメカのものであることを公開鍵証明書認証局CAが証明する書類であるデスクランブラ用公開鍵証明書Cert\_\_iを予め記憶する。このデスクランブラ用公開鍵証明書Cert\_\_iは、図4に示されるように、デスクランブラ260（プレーヤメカ）のID（証明書のシリアル番号）や、デスクランブラ用秘密鍵SK\_\_iに対するデスクランブラ用公開鍵PK\_\_i、デスクランブラ用公開鍵PK\_\_iに対する証明書認証局CAの署名、（証明書の）有効期限等から構成される。

【0054】乱数生成部274は、時変の値として乱数（例えば、128bit）を生成する。

【0055】公開鍵無効化リストチェック部275は、公開鍵無効化リストCRLに相手（ICカード210a）のIDが含まれているか否かチェックする。

【0056】楕円曲線暗号処理部276は、SACにおける認証等の際に、楕円曲線にしたがった暗号処理（例えば、256bitの処理単位）を実行する。

【0057】認証部277は、SACを介してICカード210aと通信する通信インタフェースである。

【0058】バッファメモリ278は、乱数生成部274が生成した乱数や、楕円曲線暗号処理部276が生成した一時的なデータを保持する。

【0059】次いで、ICカード210aおよびデスクランブラ260間のSAC設定、並びに、DVD2aに記録された暗号化コンテンツを復号化のシーケンスを図5に基づいて説明する。図5は、ICカード210aおよびデスクランブラ260により行われる通信シーケン



ス図である。

【0060】ユーザ操作によるDVD2aのコンテンツ再生指示があると、デスクランブラ260の乱数生成部274は、第1の乱数 $y$ （例えば、128ビット）を生成し、これをバッファメモリ278に格納する（S1）。そして、デスクランブラ260の認証部277は、バッファメモリ278に格納された第1の乱数 $y$ と、デスクランブラ用公開鍵証明書記憶部273に記憶されたデスクランブラ用公開鍵証明書 $Cert\_i$ とを読み出して、これらをICカード210aに送信する（S2）。

【0061】ICカード210aの認証部237は、デスクランブラ260から受信した第1の乱数 $y$ とデスクランブラ用公開鍵証明書 $Cert\_i$ とをバッファメモリ238に格納する。そして、公開鍵無効化リストチェック部235は、HD-DVDプレーヤ200aから渡された公開鍵無効化リストCRLに基づいて、デスクランブラ260がRevokedされていないかどうかチェックする（S3）。具体的には、公開鍵無効化リストCRLにデスクランブラ260のIDが掲載されているかどうかで判断する。Revokedされていない場合には、認証部237は、公開鍵認証局の公開鍵 $PK\_CA$ で、デスクランブラ用公開鍵証明書 $Cert\_i$ の検証を行う（S4）。具体的には、デスクランブラ用公開鍵証明書 $Cert\_i$ に含まれる公開鍵認証局の署名を公開鍵認証局の公開鍵 $PK\_CA$ で解読し、デスクランブラ用公開鍵証明書 $Cert\_i$ が確かにデスクランブラ260のものであるかどうか検証する。検証が終わると、乱数生成部234は、第1の乱数 $x$ （例えば、128ビット）を生成し、生成した第1の乱数 $x$ をバッファメモリ238に格納する（S5）。そして、認証部237は、バッファメモリ238に格納された第1の乱数 $x$ と、ICカード用公開鍵証明書記憶部233に記憶されたICカード用公開鍵証明書 $Cert\_A$ とを読み出して、これらをデスクランブラ260に送信する（S6）。

【0062】デスクランブラ260においては、ICカード210aから受信した第1の乱数 $x$ と、ICカード用公開鍵証明書 $Cert\_A$ とを、認証部277によりバッファメモリ278に格納させた後、公開鍵無効化リストチェック部275は、HD-DVDプレーヤ200aから渡された公開鍵無効化リストCRLに基づいて、ICカード210aがRevokedされていないかどうかをチェックする（S7）。具体的には、公開鍵無効化リストCRLにICカード210aのIDが掲載されているかどうかで判断する。Revokedされていない場合には、認証部277は、公開鍵証明書認証局の公開鍵 $PK\_CA$ を用いて、ICカード用公開鍵証明書 $Cert\_A$ の検証を行う（S8）。具体的には、プレーヤメーカ用公開鍵証明書 $Cert\_A$ に含まれる公開鍵認証局の署名を公開鍵認証局の公開鍵 $PK\_CA$ で解読し、I

Cカード用公開鍵証明書 $Cert\_A$ が確かにICカード210aのものであるかどうか検証する。検証が終わると乱数生成部274は、第2の乱数 $y'$ （例えば、128ビット）を生成し、この第2の乱数 $y'$ をバッファメモリ278に格納する（S9）。そして、楕円曲線暗号処理部276は、第2の乱数 $y'$ とベースポイント $G$ （定数）とを楕円曲線上で乗算し、乗算の結果 $y'G$ を生成し、この乗算の結果 $y'G$ をバッファメモリ278に記憶する（S10）。次いで、認証部277は、乗算の結果 $y'G$ に対する署名 $S1 := Sig(SK\_i, y'G || x)$ を生成し、この署名 $S1$ をバッファメモリ278に記憶する（S11）。この署名は、乗算の結果 $y'G$ に第1の乱数 $x$ をビット連結したものに対して、秘密鍵 $SK\_i$ で署名することにより行われる。なお、記号「||」は、ビット連結を表し、 $y'G$ と、乱数 $x$ を桁方向に結合して256ビット（例えば、 $y'G$ を上位128ビット、乱数 $x$ を下位128ビット）とすることを示している。署名 $S1$ の記憶が終わると、認証部277は、乗算結果 $y'G$ と、これに対する署名 $S1$ とをICカード210aに送る（S12）。

【0063】ICカード210aの認証部237は、 $y'G$ と、これに対する署名 $S1$ とをバッファメモリ238に記憶した後、デスクランブラ用公開鍵証明書 $Cert\_i$ により入手したデスクランブラ用公開鍵 $PK\_i$ を用いて、 $S1$ が $y'G || x$ に対するデスクランブラ260の署名であることを検証する（S13）。具体的には署名 $S1$ をデスクランブラ用公開鍵 $PK\_i$ で解読し、 $y'G$ と乱数 $x$ とのビット連結を分離したりして、検証する。これにより、通信相手（デスクランブラ260）が盗聴者等でないことを確認することができる。

【0064】このような検証が終わると、ICカード210aの乱数生成部234は、第2の乱数 $x'$ を生成し、バッファメモリ238に記憶する（S14）。次いで、楕円曲線暗号処理部236は、第2の乱数 $x'$ とベースポイント $G$ （定数）とを楕円曲線上で乗算し、乗算の結果 $x'G$ を生成し、これをバッファメモリ238に記憶する（S15）。次いで、認証部237は、乗算の結果 $x'G$ に対する署名 $S0 := Sig(SK\_A, x'G || y)$ を生成し、この署名 $S0$ をバッファメモリ238に記憶する（S16）。この署名は、乗算の結果 $x'G$ に第1の乱数 $y$ をビット連結したものを、秘密鍵 $SK\_A$ で署名することにより行われる。署名の記憶が終わると、認証部237は、乗算結果 $x'G$ と署名 $S0$ とをデスクランブラ260に送る（S17）。

【0065】デスクランブラ260の認証部277は、ICカード210aから受け取った乗算結果 $x'G$ と署名 $S0$ とをバッファメモリ278に記憶させた後、ICカード用公開鍵証明書 $Cert\_A$ により入手したICカード用公開鍵 $PK\_A$ を用いて、 $S0$ が $x'G || y$ に対するデスクランブラ260の署名であることを検証す



る(S18)。具体的には署名S1をデスクランブラ用公開鍵PK<sub>i</sub>で読解し、y'・Gと乱数xとのビット連結を分離したりして、検証する。これにより、通信相手(ICカード210a)が盗聴者等でないことを確認することができる。

【0066】デスクランブラ260の認証部277は、ICカード210aがRevokeされておらず、盗聴者等でもないことの確認が済むと、バッファメモリ278に記憶した自己側で生成した第2の乱数y' (例えば、128ビット)と、通信相手からもらった乗算結果x'・Gとの乗算K'=y'・(x'・G)を計算により生成し、計算結果K'をセッション鍵としてバッファメモリ278に格納する(S19)。

【0067】一方、ICカード210aの認証部237は、デスクランブラ260がRevokeされておらず、盗聴者等でもないことの確認が済むと、バッファメモリ238に記憶されている自己側で生成した第2の乱数x'と、通信相手からもらった乗算結果y'・Gとの乗算K:=x'・(y'・G)を計算により生成し、計算結果Kをセッション鍵としてバッファメモリ238に格納する(S20)。これにより、ICカード210aとデスクランブラ260とは、同じ値の鍵K(=K')を持ち合うことができ、以降、K(=K')をセッション鍵として、暗号通信を行う(S21)。

【0068】セッション鍵Kの生成が終わると、ICカード210aのコンテンツ鍵復号部220aは、コンテンツ鍵復号化処理を実行する。このコンテンツ鍵復号化処理においては、先ずハッシュ関数処理部222は、HD-DVDプレーヤ200aから渡された公開鍵無効化リストCRLのハッシュ値Hashを計算する(S22)。次いで、Ex-OR部223は、証明書認証局用公開鍵記憶部231に記憶されたICカード210a自身のデバイス鍵KD\_Aとハッシュ値Hashとの排他的論理和をとる(S23)。Dec処理部224は、得られた排他的論理和値で、暗号化コンテンツ鍵を復号化し、コンテンツ鍵Kcを取得し(S24)、このコンテンツ鍵Kcを認証部237に渡してコンテンツ鍵復号化処理を終了する。認証部237は、コンテンツ鍵Kcが渡されると、このコンテンツ鍵Kcをセッション鍵Kで暗号化し(S25)、SAC経由で、デスクランブラ260に送信する(S26)。これにより、コンテンツ鍵Kcの盗聴等が確実に防がれる。

【0069】デスクランブラ260の認証部277は、ICカード210aから受信した暗号化コンテンツ鍵をセッション鍵K'で復号化し、コンテンツ鍵Kcを取得し(S27)、取得したコンテンツ鍵KcをDec処理部280に渡す。デスクランブラ260は、暗号化されたコンテンツを認証部277から渡されたコンテンツ鍵Kcで復号化し、コンテンツを取得する(S28)。これにより、著作権保護を図りつつコンテンツの復号化が

可能になる。

【0070】ここで、ICカード210a、デスクランブラ260に対して、HD-DVDプレーヤ200aが、DVD2aにバインドされた公開鍵証明書無効化リストCRLの代わりに、自己の公開鍵が無効になる前の公開鍵証明書無効化リストCRLにすり替えて渡した場合を想定する。この場合には、すり替えがなかった場合と同様に、SAC設定がされ、セッション鍵による暗号通信の段階(S21)までは進むことができる。

10 【0071】しかしながら、本実施の形態1では、公開鍵証明書無効化リストCRLと、この公開鍵証明書無効化リストCRLのハッシュ値Hashを関与させた情報で暗号化された暗号化コンテンツ鍵の束とをDVD2aにバインドするようにしている。このため、CRLのすり替えが行われたような場合、すり替えた公開鍵証明書無効化リストCRLのハッシュ値HashとDVD2aにバインドされた公開鍵証明書無効化リストCRLのハッシュ値Hashとは、その値が一致しない。この結果、すり替えた公開鍵証明書無効化リストCRLのハッシュ値Hashを用いてコンテンツ鍵を復号しようとしても、正規のコンテンツ鍵Kcを取得できない。このため、コンテンツを復号するためのコンテンツ鍵Kcを得るためには、DVD2aにバインドされた公開鍵証明書無効化リストCRLを渡さなければならなくなる。したがって、公開鍵証明書無効化リストCRLのすり替えを行うような悪質な復号化装置200aを排除することができ、著作権の保護を強化することができる。

20 30 【0072】(実施の形態2)図6は、本実施の形態2に係る記録メディア用著作権保護システム1bの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム1bにおいて、実施の形態1の記録メディア用著作権保護システム1aと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム1aの場合との異同を中心に説明する。

40 【0073】実施の形態1に係る暗号化装置100aの端末装置110aでは、ハッシュ関数処理部114から出力された公開鍵証明書無効化リストCRLのハッシュ値Hashと各デバイス鍵との排他的論理和値をEx-OR部115により算出し、Enc部116において、コンテンツ鍵Kcをその排他的論理和値で暗号化し、暗号化コンテンツ鍵の束を生成していた。これに対して実施の形態2の暗号化装置100bの端末装置110bにおいては、Enc部117においてコンテンツ鍵Kcをデバイス鍵束記憶部112に記憶された各デバイス鍵だけで暗号化し、各デバイス鍵だけで暗号化された暗号化コンテンツ鍵の束を生成するように構成されている。

50 【0074】また、実施の形態1に係る暗号化装置100aの端末装置110aは、コンテンツ鍵Kcをそのまま端末装置160に渡していた。このため、端末装置1



60では、Enc部162においてコンテンツをコンテンツ鍵Kcで暗号化し、暗号化コンテンツを生成していた。これに対して、実施の形態2の暗号化装置100bの端末装置110bにおいては、Ex-OR部118により、ハッシュ関数処理部114から出力された公開鍵証明書無効化リストCRLのハッシュ値Hashとコンテンツ鍵Kcとの排他的論理和をとり、その排他的論理和値を端末装置160に渡すように構成されている。このため、その排他的論理和値を受け取った端末装置160では、Enc部162においてコンテンツをその排他的論理和値で暗号化し、暗号化コンテンツを生成する。

【0075】したがって、DVD2bにバインドされた各暗号化コンテンツ鍵にはハッシュ値が関与しておらず、暗号化コンテンツにはハッシュ値が関与しており、DVD2aの場合と逆の関係となる。また、実施の形態1に係る復号化装置200aのコンテンツ鍵復号部220aでは、Ex-OR部223においてデバイス鍵記憶部221に記憶された自己のデバイス鍵KD\_Aと公開鍵証明書無効化リストCRLのハッシュ値Hashとの排他的論理和値を算出し、Dec処理部224において、ハッシュ値が関与した暗号化コンテンツ鍵をその排他的論理和値で復号し、コンテンツ鍵Kcを取得していた。

【0076】これに対して、実施の形態2に係る復号化装置200bのコンテンツ鍵復号部220bでは、DVD2bにバインドされた暗号化コンテンツ鍵にハッシュ値Hashが関与していないため、Dec処理部225において暗号化コンテンツ鍵をデバイス鍵記憶部221に記憶された自己のデバイス鍵だけで復号化し、コンテンツ鍵Kcを取得するように構成されている。そして、DVD2bにバインドされた暗号化コンテンツにハッシュ値Hashが関与しているため、Ex-OR部226において、Dec処理部225により取得されたコンテンツ鍵Kcと、ハッシュ関数処理部222により算出された公開鍵証明書無効化リストCRLのハッシュ値Hashとの排他的論理和値を算出し、得られた排他的論理和値を認証処理部230aの認証部237に渡すように構成されている。

【0077】このコンテンツ鍵Kcと、ハッシュ値Hashとの排他的論理和値は、認証部237から、SAC、デスクランブラ260の認証部277を介してDec処理部280に渡される。このため、Dec処理部280は、DVD2bに記録されたハッシュ値Hashが関与した暗号化コンテンツを、コンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値で復号化し、コンテンツを取得する。

【0078】したがって、この実施の形態2に係る記録メディア用著作権保護システム1bにおいても、実施の形態1の場合と同様に、コンテンツを復号するための鍵を得るためには、DVD2aにバインドされた公開鍵証

明書無効化リストCRLを渡さなければならなくなる。この結果、公開鍵証明書無効化リストCRLのすり替えを行うような不正な復号化装置200bを排除でき、著作権の保護を強化することができる。

【0079】（実施の形態3）図7は、本実施の形態3に係る記録メディア用著作権保護システム1cの全体構成を示す機能ブロック図である。なお、同図においては、実施の形態1の記録メディア用著作権保護システム1aと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム1cに特有の機能部分のみが図示されている。

【0080】実施の形態1に係る復号化装置200cのICカード210aは、取得したコンテンツ鍵Kcをデスクランブラ260bに単純に渡すだけであり、ICカード210a自身では、取得したコンテンツ鍵Kcが暗号化コンテンツを正常に復号化できる正規の鍵かどうかはわからなかった。このため、取得したコンテンツ鍵Kcをデスクランブラ260に渡す前に、この内部でコンテンツ鍵Kcが正しい値であるかどうかを予めチェックすることが望ましい。

【0081】そこで、この本実施の形態3に係る記録メディア用著作権保護システム1cは、このような鍵チェック機能を有するシステムであって、暗号化装置100cの著作権保護ライセンスが使用する端末装置110cは、端末装置110aの構成に加えて、さらに、固定パターン記憶部119を備える。この固定パターン記憶部119は、予め定められた固定パターン平文（例えば、16進で表される固定パターン平文「0123456789ABCDEF」）をコンテンツ鍵Kcで暗号化した固定パターンを予め記憶する。この固定パターン記憶部119に記憶された固定パターンは、端末装置160を介してDVD2cにバインドされる。

【0082】その一方、復号化装置200cのICカード210cに設けられるコンテンツ鍵復号部220cは、コンテンツ鍵復号部220aの構成に加えてさらにDec処理部227と、コンテンツ復号鍵チェック部228とを備える。Dec処理部227は、DVD2aにバインドされた固定パターン平文の暗号化データをDec処理部224により復号化されたコンテンツ鍵Kcで復号化する。コンテンツ復号鍵チェック部228は、上記の固定パターン平文「0123456789ABCDEF」を予め保持しており、予め保持している固定パターン平文と、Dec処理部227により復号化された固定パターン平文とが同じであるか否かで復号化されたコンテンツ鍵Kcが正しい値であるかどうかをチェックする。

【0083】このように構成された記録メディア用著作権保護システム1cによれば、ICカード210cの内部でコンテンツ鍵Kcが正しい値であるかどうかを予めチェックすることができ、デスクランブラ260におけ



る誤ったコンテンツ鍵Kcを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。なお、この実施の形態3の記録メディア用著作権保護システム1cにおいては、鍵チェック機能を実施の形態1の記録メディア用著作権保護システム1aに適用したが、実施の形態2に係る記録メディア用著作権保護システム1bに適用してもよい。

【0084】その場合には、コンテンツがコンテンツ鍵Kcと公開鍵証明書無効化リストCRLのハッシュ値Hashとの排他的論理和値で暗号化されているので、固定パターン記憶部119に固定パターン平文「0123456789ABCDEF」をコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値で暗号化した固定パターンを予め記憶し、この固定パターンをDVD2cに記録すればよい。

【0085】一方、コンテンツ鍵復号部220cのDec処理部227では、Dec処理部224の出力、すなわちコンテンツ鍵Kcに代えてEx-OR部226（図6参照）の出力、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値でDVD2aにバインドされた固定パターン平文の暗号化データを復号化すればよい。そして、コンテンツ鍵チェック部228で、予め保持している固定パターン平文「0123456789ABCDEF」と、Dec処理部227により復号化された固定パターン平文とが同じであるか否かで復号化されたコンテンツを復号するための鍵、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値が正しい値であるかどうかをチェックできる。

【0086】（実施の形態4）図8は、本実施の形態4に係る記録メディア用著作権保護システム1dの全体構成を示す機能ブロック図である。なお、同図においても、実施の形態1の記録メディア用著作権保護システム1aと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム1dに特有の機能部分のみが図示されている。

【0087】本実施の形態4に係る記録メディア用著作権保護システム1dは、記録メディア用著作権保護システム1cと同様に鍵チェック機能を有するシステムであって、暗号化装置100dの端末装置110dは、端末装置110aの構成に加えて、さらに、Enc部131を備える。このEnc部131は、コンテンツ鍵記憶部113から読み出されたコンテンツ鍵Kcをこのコンテンツ鍵Kcで暗号化したコンテンツ鍵照合データを生成する。このコンテンツ鍵照合データは、DVD2dにバインドされる。

【0088】一方、復号化装置200dのICカード210dに設けられるコンテンツ鍵復号部220dは、コンテンツ鍵復号部220aの構成に加えてさらにEnc部241と、コンテンツ鍵チェック部242とを備える。Enc部241は、端末装置110dのEnc部1

31と同構成であって、Dec処理部224により復号化されたコンテンツ鍵Kcを、そのコンテンツ鍵Kcで暗号化し、コンテンツ鍵照合データを生成する。コンテンツ鍵チェック部242は、Enc部241により生成されたコンテンツ鍵照合データと、DVD2dにバインドされたコンテンツ鍵照合データとを比較し、これらのデータが同じ値であるか否かで、Dec処理部224により復号化されたコンテンツ鍵Kcが正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックする。

【0089】このように構成された記録メディア用著作権保護システム1dによっても、記録メディア用著作権保護システム1cと同様に、ICカード210dの内部でコンテンツ鍵Kcが正しい値であるかどうかを予めチェックすることができ、デスクランブラ260における誤ったコンテンツ鍵Kcを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。なお、この実施の形態4の記録メディア用著作権保護システム1dにおいては、鍵チェック機能を実施の形態1の記録メディア用著作権保護システム1aに適用したが、実施の形態2に係る記録メディア用著作権保護システム1bに適用してもよい。

【0090】その場合には、コンテンツがコンテンツ鍵Kcと公開鍵証明書無効化リストCRLのハッシュ値Hashとの排他的論理和値で暗号化されているので、Enc部131においては、コンテンツ鍵記憶部113の出力、すなわちコンテンツ鍵Kcに代えて、Ex-OR部118の出力、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値をこの排他的論理和値で暗号化し、このコンテンツ鍵照合データをDVD2cに記録すればよい。

【0091】一方、コンテンツ鍵復号部220dのEnc部241では、Dec処理部224の出力、すなわちコンテンツ鍵Kcに代えてEx-OR部226（図6参照）の出力、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値をその排他的論理和値で暗号化すればよい。そして、コンテンツ鍵チェック部242で、Enc部241により生成されたコンテンツ鍵照合データと、DVD2dにバインドされたコンテンツ鍵照合データとを比較し、これらの鍵が同じ値であるか否かで、Ex-OR部226により生成された鍵が正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックすることができる。

【0092】（実施の形態5）図9は、本実施の形態5に係る記録メディア用著作権保護システム1eの全体構成を示す機能ブロック図である。なお、同図においても、実施の形態1の記録メディア用著作権保護システム1aと対応する機能部分の図示が省略され、この記録メディア用著作権保護システム1eに特有の機能部分のみが図示されている。



【0093】本実施の形態5に係る記録メディア用著作権保護システム1eは、記録メディア用著作権保護システム1c、1dと同様に鍵チェック機能を有するシステムであって、実施の形態4と同じ構成の暗号化装置100dで構成されており、DVD2dには、Enc部131により生成されたコンテンツ鍵照合データがバインドされている。

【0094】一方、復号化装置200eのICカード210eに設けられるコンテンツ鍵復号部220eは、コンテンツ鍵復号部220aの構成に加えてさらにDec処理部243と、コンテンツ鍵チェック部244とを備える。Dec処理部243は、上記のEnc部131により暗号化され、DVD2dにバインドされたコンテンツ鍵照合データをDec処理部224により復号化されたコンテンツ鍵Kcで復号化する。コンテンツ鍵チェック部244は、Dec処理部224により復号化されたコンテンツ鍵Kcと、Dec処理部243により復号化されたコンテンツ鍵Kcとを比較し、これらの鍵が同じ値であるか否かで、Dec処理部224により復号化されたコンテンツ鍵Kcが正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックする。

【0095】このように構成された記録メディア用著作権保護システム1eによっても、メディア用著作権保護システム1c、1dと同様に、ICカード210eの内部でコンテンツ鍵Kcが正しい値であるかどうかを予めチェックすることができ、デスクランブラ260における誤ったコンテンツ鍵Kcを用いたコンテンツ復号化という無駄な復号化処理を事前に回避することができる。

【0096】なお、この実施の形態5の記録メディア用著作権保護システム1eにおいては、鍵チェック機能を実施の形態1の記録メディア用著作権保護システム1aに適用したが、実施の形態2に係る記録メディア用著作権保護システム1bに適用してもよい。

【0097】この場合には、コンテンツがコンテンツ鍵Kcと公開鍵証明書無効化リストCRLのハッシュ値Hashとの排他的論理和値で暗号化されているので、実施の形態4の変形例と同様に、Enc部131においては、コンテンツ鍵記憶部113の出力、すなわちコンテンツ鍵Kcに代えて、Ex-OR部118の出力、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値をこの排他的論理和値で暗号化し、この暗号化により生成されたコンテンツ鍵照合データをDVD2cに記録すればよい。

【0098】一方、コンテンツ鍵復号部220eのDec処理部243では、DVD2cから読み出したコンテンツ鍵復号データを、Dec処理部224の出力、すなわちコンテンツ鍵Kcに代えてEx-OR部226（図6参照）の出力、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和値で復号化する。そして、

コンテンツ復号鍵チェック部244において、Ex-OR部226により復号化されたコンテンツを復号化するための鍵、すなわちコンテンツ鍵Kcとハッシュ値Hashとの排他的論理和と、Dec処理部243により復号化された鍵とを比較し、これらの鍵が同じ値であるか否かで、Ex-OR部226により復号化された鍵が正しい鍵、すなわち暗号化コンテンツを復号できる鍵であるかどうかをチェックすればよい。

【0099】（実施の形態6）図10は、本実施の形態6に係る記録メディア用著作権保護システム1fの全体構成を示す機能ブロック図である。上述の記録メディア用著作権保護システム1a～1eでは、DVDにバインドされた公開鍵証明書無効化リストCRLを公開鍵無効化リストチェック部235でチェックし、通信相手（デスクランブラ260）がRevokeされているか否か判断していた。このようなチェックでは、DVDの製造時期が古い、すなわちDVDにバインドされた公開鍵証明書無効化リストCRLが古いと、この公開鍵証明書無効化リストCRLの更新日以降に通信相手（デスクランブラ260）の公開鍵証明書が無効化されたような場合、このデスクランブラ260をRevokeすることができない。このため、できるだけ最新版の公開鍵証明書無効化リストCRLを使用して、通信相手（デスクランブラ260）がRevokeされているか否か判断する必要がある。

【0100】そこで、この本実施の形態6に係る記録メディア用著作権保護システム1fにおいては、復号化装置200fのICカード210fに係る認証処理部230bに、認証処理部230aの構成に加えてさらに公開鍵無効化リスト最新版記憶処理部239が設けられている。

【0101】この公開鍵無効化リスト最新版記憶処理部239は、今までに受け取った公開鍵証明書無効化リストCRL中の最新版を復号化装置200f側で記憶して保持するための処理部であって、最新版検出処理部2391と、最新版検出情報記憶部2392と、記憶部2393等とからなる。

【0102】最新版検出処理部2391は、DVD2aにバインドされた公開鍵証明書無効化リストCRLを受け取るごとに、この公開鍵証明書無効化リストCRLが最新版か否かの確認判断の処理等を行う。

【0103】最新版検出情報記憶部2392は、この復号化装置200f側で保持する公開鍵証明書無効化リストCRLの最新版検出情報（例えば、このリストのファイルサイズ）を記憶する。

【0104】記憶部2393は、復号化装置200f側で保持する公開鍵証明書無効化リストCRLのハッシュ値（例えば、128ビット）を記憶する。その理由は、膨大な量となる公開鍵証明書無効化リストCRL自体をICカード210f内で記憶・保持したのでは、ICカ



ード210fのコストアップになり得るので、それを回避するためにである。つまり、この実施の形態では、ICカード210fの外（かつ、復号化装置200fの中）に、公開鍵証明書無効化リスト最新版記憶部250を設け、この公開鍵証明書無効化リスト最新版記憶部250に最新版の公開鍵証明書無効化リストCRL本体を記憶させ、このリストのハッシュ値だけをICカード210f内の記憶部2393で記憶・保持する構成を採用している。そして、公開鍵無効化リストチェック部235により通信相手が無効化されている機器かどうかのチェックを行う場合に、最新版の公開鍵証明書無効化リストCRLをICカード210f内に読み出し、読み出した公開鍵証明書無効化リストCRLが改ざんされていないかをハッシュ値でチェックしている。

【0105】具体的には、DVD2aにバインドされた新たな公開鍵証明書無効化リストCRLを受け取ると、その公開鍵証明書無効化リストCRLを保存しておく

（又は、保存しないでおく）ための処理として、最新版検出処理部2391は、先ず、図11（a）のフローチャートに示されるように、公開鍵証明書無効化リストCRLが最新版か否かの確認判断の処理を実行する。つまり、最新版検出処理部2391は先ず、DVD2aにバインドされた公開鍵証明書無効化リストCRLのヘッダに記録されたファイルサイズと、最新版検出情報記憶部2392に記憶しているファイルサイズとを比較する

（S101）。この比較は、時が経つにつれて無効化される機器の台数が単調増加するだけであり、ファイルサイズも大きくなるという公開鍵証明書無効化リストCRLの性質を根拠としている。

【0106】その結果、DVD2aにバインドされた公開鍵証明書無効化リストCRLのファイルサイズの方が大きい場合（S101でYes）、すなわち、今DVD2aから読み込んだ公開鍵証明書無効化リストCRLの方が最新である場合、この最新版リストのファイルサイズを最新版検出情報記憶部2392に格納（上書き）して更新する（S102）。次いで最新版検出処理部2391は、最新版リストのハッシュ値を算出して、算出したハッシュ値を記憶部2393に格納し（S103）、最新版リストを外部の公開鍵証明書無効化リスト最新版記憶部250に格納し（S104）、公開鍵無効化リストチェック部235に最新版リストを転送して（S105）、確認判断処理を終了する。

【0107】一方、DVD2aにバインドされた公開鍵証明書無効化リストCRLのファイルサイズの方が大きい場合（S101でNo）、すなわち、今DVD2aから読み込んだ公開鍵証明書無効化リストCRLの方が最新でない場合、最新版検出処理部2391は、確認判断処理を直ちに終了する。そして、もし、最新の公開鍵証明書無効化リストCRLが必要な場合には、図11（b）のフローチャートに示される最新版リスト読み出

し処理を実行する。

【0108】その読み出し処理においては、最新版検出処理部2391は、先ず、最新版リストを外部の記憶部、すなわち公開鍵証明書無効化リスト最新版記憶部250から読み出し（S111）、最新版リストのハッシュ値を算出し（S112）、算出したハッシュ値と記憶部2393に記憶されているハッシュ値とが一致するか否かを判断する（S113）。この判断は、公開鍵証明書無効化リストCRLがICカード210fの外部ですり替えが行われたか否かを検出するために行われ、すり替えがなかった場合には、ハッシュ値は一致する。

【0109】ハッシュ値が一致する場合（S113でYes）、最新版検出処理部2391は、公開鍵証明書無効化リスト最新版記憶部250から読み出した最新版リストを公開鍵無効化リストチェック部235に転送して（S114）、最新版リスト読み出し処理を終了する。これに対してハッシュ値が一致しない場合（S113でNo）、最新版検出処理部2391は、処理を中止して（S115）、最新版リスト読み出し処理を終了する。

なお、ハッシュ値が一致しないために最新の公開鍵証明書無効化リストCRLを読み出すことができなかった場合には、何らかの不正行為が行われたものとして、例えば、公開鍵証明書無効化リストCRLを用いる以降の全ての処理を中止（相手装置の認証を拒絶）する。

【0110】このように、実施の形態6の記録メディア用著作権保護システム1fによれば、DVD2aから読み出された公開鍵証明書無効化リストCRLのうち、最新のものだけが公開鍵証明書無効化リスト最新版記憶部250に保持され、利用されるので、古い公開鍵証明書無効化リストCRLを用いて相手装置を認証してしまう不具合が回避される。なお、この実施の形態6においては、最新版リストの確認方法としてファイルサイズを用いたが、この変形例として、公開鍵証明書無効化リストCRLに登録されている証明書の件数（シリアル番号のエントリー数）で最新版リストか否かの確認をしてもよい。

【0111】次に、本発明に係る著作権保護システムの実施の形態である記録媒体用の復号化装置200a～200fをHD-DVDプレーヤに適用した例について、図面を用いて説明する。図12は、本発明の実施の形態に係る記録媒体用の復号化装置200a～200fを備えるHD-DVDプレーヤの外観図である。このHD-DVDプレーヤ200は、DVD2a～2dに記録された映画等のコンテンツをICカード210a～210fを用いて再生するシステムであり、ICカード210a～210fが装着されるカード挿入口2100、DVD2a～2dを再生するDVD-ROMドライブ2200、HD-DVDプレーヤ200の本体内部に実装されるデスクランブラ260等から構成される。

【0112】なお、ICカード210a～210fは、



プラスチック製のカードにCPUを含むICチップが埋め込まれたカードであり、内蔵されたCPUによる処理により、データの読み書きの際のアクセスが正当なものであるかどうかを判断できる。そのため、外部からの不正なアクセスや改ざんを行うことが非常に困難であり、高いセキュリティを実現できる。

【0113】本発明に係る暗号化装置をこのような映像再生システムに適用することで、DVD2a～2dに記録されたデジタル著作物は不正コピー等から保護され、マルチメディア関連製品の流通市場における健全な発展が期待できる。

【0114】（実施の形態7）図13は、本実施の形態7に係る記録メディア用著作権保護システム1gの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム1gにおいて、実施の形態1の記録メディア用著作権保護システム1aと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム1aとの異同を中心に説明する。

【0115】ところで、実施の形態1に係る暗号化装置100aでは、2つの鍵、デバイス鍵KD\_Aの束と、コンテンツ鍵Kcとをデバイス鍵束記憶部112、コンテンツ鍵記憶部113にそれぞれ記憶しておき、コンテンツ鍵Kcを、公開鍵無効化リストCRLのハッシュ値を関与させたデバイス鍵KD\_Aの束で暗号化し、暗号化コンテンツ鍵の束を生成し、コンテンツをコンテンツ鍵Kcで暗号化し、暗号化コンテンツ鍵を生成していた。すなわち、デバイス鍵KD\_Aと、コンテンツ鍵Kcとで、秘密鍵を2層化している。このような秘密鍵の2層化で、通常は、アタックに対する暗号強度が十分にある。

【0116】しかしながら、暗号強度をさらに向上させて欲しいというライセンサもある。そこで、本実施の形態7の暗号化装置100eの端末装置110eにおいては、秘密鍵を上記したデバイス鍵KD\_Aおよびコンテンツ鍵Kcに、ディスク鍵Kdをさらに加えた3層化した構成を採用し、暗号強度をさらに向上させている。

【0117】すなわち、暗号化装置100eの端末装置110eは、公開鍵無効化リスト記憶部111、デバイス鍵束記憶部112、コンテンツ鍵記憶部113、ハッシュ関数処理部114、Ex-OR部115の他に、さらに、ディスク鍵Kdを予め記憶するハッシュ関数処理部114と、Enc部142、143とを備えている。なお、このディスク鍵Kdは、1枚のDVDに複数（7個程度）のコンテンツが入ることを考慮し、コンテンツごとのコンテンツ鍵の上位に設けられる秘密鍵である。

【0118】Enc部142は、ディスク鍵記憶部141に記憶されたディスク鍵Kdをハッシュ値Hashと各デバイス鍵KD\_Aとの排他的論理和値で暗号化し、暗号化ディスク鍵の束を生成する。

【0119】Enc部143は、コンテンツ鍵記憶部1

13に記憶されたコンテンツ鍵Kcをディスク鍵Kdで暗号化し、暗号化コンテンツ鍵を生成する。

【0120】このため、端末装置160は、DVD2eに対して、暗号化コンテンツや、公開鍵証明書無効化リストCRLの他、上記Enc部142、143により生成された暗号化ディスク鍵の束と、暗号化コンテンツ鍵とをバインドさせる。これに応じて、復号化装置200gのICカード210gのコンテンツ鍵復号部220fは、デバイス鍵KD\_Aだけを記憶し、DVD2eにバインドされた暗号化ディスク鍵の束をデバイス鍵KD\_Aと公開鍵無効化リストCRLのハッシュ値とで復号化することにより、ディスク鍵Kdを復号化し、さらに、DVD2eにバインドされた暗号化コンテンツ鍵をディスク鍵Kdで復号化することにより、コンテンツ鍵Kcを復号化する。すなわち、コンテンツ鍵復号部220fは、デバイス鍵記憶部221、ハッシュ関数処理部222、Ex-OR部223の他に、Dec処理部245、246を備えている。

【0121】Dec処理部245は、デスクランブラ260から渡された暗号化ディスク鍵の束をデバイス鍵KD\_Aと公開鍵無効化リストCRLのハッシュ値とで復号化することにより、ディスク鍵Kdを復号化する。

【0122】Dec処理部246は、デスクランブラ260から渡された暗号化コンテンツ鍵をディスク鍵Kdで復号化することにより、コンテンツ鍵Kcを復号化する。したがって、この実施の形態7に係る記録メディア用著作権保護システム1gにおいても、実施の形態1の場合と同様に、コンテンツを復号するための鍵を得るためには、DVD2eにバインドされた公開鍵証明書無効化リストCRLを渡さなければならなくなり、公開鍵証明書無効化リストCRLのすり替えを行うような不正なデスクランブラ260を排除できるだけでなく、秘密鍵が3層化されているので、アタックに対する暗号強度が増加し、さらに著作権の保護を強化することができる。なお、この実施の形態では、秘密鍵を3層化したか、さらに多層化する構成で実施してもよい。この場合には、アタックに対する暗号強度をさらに増加させることができる。

【0123】また、端末装置110eに、さらに、復号化装置200gにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをDVD2eに出力する確認データ出力部を備える構成としてもよい。この確認データ出力部は、所定の固定パターンのデータをコンテンツ鍵記憶部113に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2eに出力する構成であってもよく、また、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2eに出力する構成でもよい。また、この端末装置110eに対応して、コンテンツ鍵復号部220f



に、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部228、コンテンツ鍵チェック部242、コンテンツ復号鍵チェック部244等を備える構成としてもよい。

【0124】（実施の形態8）図14は、本実施の形態8に係る記録メディア用著作権保護システム1hの全体構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム1hにおいて、実施の形態7の記録メディア用著作権保護システム1gと対応する部分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム1gとの異同を中心に説明する。

【0125】ところで、実施の形態7に係る暗号化装置100eの端末装置110eでは、ディスク鍵記憶部141に記憶されたディスク鍵Kdをハッシュ値Hashと各デバイス鍵KD\_Aとの排他的論理和値で暗号化し、暗号化ディスク鍵の束を生成するとともに、コンテンツ鍵記憶部113に記憶されたコンテンツ鍵Kcをディスク鍵Kdで暗号化し、暗号化コンテンツ鍵を生成する。この結果、端末装置110eでは、アタックに対する暗号強度が増加する反面、2つの暗号化処理のための負荷が大きい。また、コンテンツ鍵復号部220fにおいても、2つの復号化処理のための負荷も大きい。

【0126】そこで、本記録メディア用著作権保護システム1hの暗号化装置100fに係る端末装置110fでは、コンテンツ鍵記憶部113に代えてDVDごとに固有のメディアID、MIDを記憶するメディアID記憶部144と、Enc部143に代えてメディアID、MIDとディスク鍵Kdとに基づいてコンテンツ鍵Kcを生成する一方向関数部145とを用い、コンテンツ鍵Kcを暗号化する処理を省くことにより、端末装置110fの付加の軽減を図っている。すなわち、暗号化装置100fの端末装置110fは、公開鍵無効化リスト記憶部111、デバイス鍵束記憶部112、ハッシュ関数処理部114、Ex-OR部115、ディスク鍵記憶部141、Enc部142の他に、さらにメディアID記憶部144と、一方向関数部145とを備えている。

【0127】一方向関数部145は、例えばEx-ORであって、メディアID記憶部144に記憶されたメディアID、MIDとディスク鍵Kdとを一方向関数に代入することにより、コンテンツ鍵Kcを生成する。このコンテンツ鍵Kcを生成する処理は、図13のEnc部143による暗号化コンテンツ鍵を生成する処理に比べて負荷が軽い。

【0128】端末装置160は、DVD2fに対して、公開鍵無効化リストCRL、暗号化コンテンツの他、上記Enc部142により生成された暗号化ディスク鍵の束と、メディアID記憶部144から出力されたメディアID、MIDとをバインドさせる。

【0129】これに応じて、復号化装置200hのICカード210hのコンテンツ鍵復号部220gは、デバ

イス鍵KD\_Aだけを記憶し、DVD2eにバインドされた暗号化ディスク鍵の束をデバイス鍵KD\_Aと公開鍵無効化リストCRLのハッシュ値とで復号化することにより、ディスク鍵Kdを復号化し、さらに、DVD2eにバインドされたメディアID、MIDとディスク鍵Kdとに基づいて、コンテンツ鍵Kcを生成する。すなわち、コンテンツ鍵復号部220gは、デバイス鍵記憶部221、ハッシュ関数処理部222、Ex-OR部223、Dec処理部245の他に、さらに一方向関数部145と同構成の一方向関数部247を備えている。

【0130】一方向関数部247は、メディアID、MIDをディスク鍵Kdで一方向関数処理することにより、コンテンツ鍵Kcを生成する。このコンテンツ鍵Kcを生成する処理は、図13のDec処理部246によるコンテンツ鍵Kcを復号化する処理に比べて負荷が軽い。ここで、メディアID、MIDはDVD2fにバインドされるので容易に知られるが、一方向関数部145、247の構成は秘密鍵と同様に知られにくい。

【0131】したがって、この実施の形態8に係る記録メディア用著作権保護システム1hにおいても、実施の形態1の場合と同様に、コンテンツを復号するための鍵を得るためには、DVD2aにバインドされた公開鍵証明書無効化リストCRLを渡さなければならなくなり、公開鍵証明書無効化リストCRLのすり替えを行うような不正なデスクランブラ260を排除できるだけでなく、暗号の強度が増すため、アタックに対する暗号強度が増加し、さらに著作権の保護を強化することができ、しかも端末装置110fおよびコンテンツ鍵復号部220gの負荷軽減することができる。

【0132】なお、端末装置110fに、さらに、復号化装置200hにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをDVD2fに出力する確認データ出力部を備える構成としてもよい。この確認データ出力部は、所定の固定パターンのデータをコンテンツ鍵記憶部113に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2fに出力する構成であってもよく、また、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2fに出力する構成でもよい。また、この端末装置110fに対応して、コンテンツ鍵復号部220fに、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部228、コンテンツ鍵チェック部242、コンテンツ復号鍵チェック部244等を備える構成としてもよい。

【0133】（実施の形態9）図15は、本実施の形態9に係る記録メディア用著作権保護システム1iの一部構成を示す機能ブロック図である。なお、この記録メディア用著作権保護システム1iにおいて、実施の形態1の記録メディア用著作権保護システム1aと対応する部



分に同じ番号を付し、その説明を省略し、記録メディア用著作権保護システム1aとの異同を中心に説明する。

【0134】ところで、DVDというメディアは、パーソナルコンピュータ（PC）でも読み込むことができ、PCとの親和性が高く、PCにDVDドライブを装着すると同時に、再生ソフトをハードディスク等にインストールしておき、このPCをHD-DVDと同様に復号化装置として使用し、コンテンツを視聴することが行われている。この場合においても、DVDドライブが不正を働く場合が考えられ、HD-DVDの場合と同様に、著作権の保護を図る必要がある。

【0135】一方、実施の形態1では、ICカード210aとデスクランブラ260とで復号化装置200aを構成していたが、PCの場合には、DVDドライブと再生ソフトとで復号化装置を構成するのか一般的である。そこで、この実施の形態9では、デスクランブラ260の認証処理部270の部分をDVDドライブ400に含ませ、ICカード210aとデスクランブラ260のDec処理部280の部分をDVD再生PCソフト500に含ませることにより、復号化装置200iを構成している。なお、DVDドライブ400の製造元とDVD再生PCソフト500の販売元とは異なる。

【0136】DVDドライブ400は、認証処理部270と略同構成であり、バス認証用公開鍵証明書記憶部410と、バス認証用秘密鍵記憶部420と、公開鍵復号部430と、鍵計算部440と、バス暗号部450とを備えている。

【0137】DVDドライブ400のバス認証用公開鍵証明書記憶部410は、IDEバスやSCSIバス等のバス認証用の公開鍵証明書を予め記憶しており、DVD2aのコンテンツ再生に際して、バス認証用の公開鍵証明書をDVD再生PCソフト500に渡す。

【0138】バス認証用秘密鍵記憶部420～バス暗号部450は、セッション鍵Kを生成し、DVD再生PCソフト500との間でSACを形成するものである。

【0139】DVD再生PCソフト500は、その機能として、証明書正当性検査部510と、公開鍵有効性検査部520と、公開鍵暗号部530と、検証部540と、鍵計算部550と、バス復号部560と、ハッシュ関数処理部570と、デバイス鍵記憶部580と、Dec処理部590、595とを備える。このような各部は、ソフトと、PCのCPU、メモリ等により実現される。

【0140】証明書正当性検査部510は、バス認証用公開鍵証明書記憶部410から送られてきた証明書を公開鍵で読解し、証明書が正当なものかどうか検査する。

【0141】公開鍵有効性検査部520は、証明書正当性検査部510から証明書が正当である旨の通知を受けると、DVDドライブ400を介して受け取ったバス認証用公開鍵無効化リストCRLと、公開鍵証明書無効化

リスト最新版記憶部250から読み出した最新のバス認証用公開鍵無効化リストCRLとを参照し、DVDドライブ400がRevokeされていないかどうか検査する。

【0142】公開鍵暗号部530～バス復号部560は、公開鍵有効性検査部520からDVDドライブ400がRevokeされていない、すなわち、DVDドライブ400が正当である旨の通知を受けると、セッション鍵K'を生成し、DVDドライブ400との間でSACを形成する部分である。

【0143】公開鍵暗号部530は、公開鍵証明書無効化リストCRLのハッシュ値Hashを算出する。

【0144】デバイス鍵記憶部580は、デバイス鍵KD\_Aを予め記憶する。

【0145】Dec処理部590は、バス復号部560から出力された暗号化コンテンツ鍵と、ハッシュ関数処理部570から出力されたハッシュ値Hashと、デバイス鍵KD\_Aとに基づいて、コンテンツ鍵Kcを生成する。Dec処理部590は、DVD2aにバインドされた暗号化コンテンツをコンテンツ鍵Kcで復号化し、コンテンツを生成する。

【0146】次いで、DVDドライブ400とDVD再生PCソフト500との間で行われる認証の処理等を説明する。公開鍵暗号部530は、DVDドライブ400が正当である旨の通知を受け取ると、乱数chaを生成し、生成した乱数chaを相手のバス認証用公開鍵で暗号化し、DVDドライブ400の公開鍵復号部430に暗号化した乱数chaを転送する。

【0147】公開鍵復号部430は、暗号化された乱数chaを、バス認証用秘密鍵記憶部420に記憶されているバス認証用秘密鍵で読解し、乱数chaを取得する。そして、公開鍵復号部430は、乱数chaと自己の秘密鍵とを相手のバス認証用公開鍵で暗号化し、暗号化結果を検証部540に転送すると共に、乱数chaと秘密鍵とを鍵計算部440に渡す。鍵計算部440は、乱数chaと秘密鍵とに基づいてセッション鍵Kを計算し、セッション鍵Kをバス暗号部450に渡す。バス暗号部450は、暗号化コンテンツ鍵の束をセッション鍵Kで暗号化し、2重に暗号化されたコンテンツ鍵の束をDVD再生PCソフト500に送る。

【0148】一方、DVD再生PCソフト500の検証部540は、自己の秘密鍵を用いて、復号により得られた乱数chaが元の乱数chaと一致するかを確認し、一致していれば、乱数chaと、相手の秘密鍵とを鍵計算部550に渡す。鍵計算部550は、乱数chaと、相手の秘密鍵とを用いてセッション鍵K'を計算し、バス復号部560に渡す。バス復号部560は、2重に暗号化されたコンテンツ鍵の束をセッション鍵K'で復号化し、暗号化コンテンツ鍵の束を生成し、暗号化コンテンツ鍵の束をDec処理部590に出力する。



【0149】他方、ハッシュ関数処理部570は、DVDドライブ400を介して出力されたCRLのハッシュ値Hashを算出し、ハッシュ値HashをDec処理部590に出力する。Dec処理部590は、例えば、暗号化コンテンツ鍵の束とハッシュ値Hashとの排他的論理和を算出することにより、コンテンツ鍵Kcをデバイス鍵KD\_Aで暗号化した値に復号化し、これをさらにデバイス鍵KD\_Aで復号化することにより、コンテンツ鍵Kcを復号化し、コンテンツ鍵KcをDec処理部595に渡す。Dec処理部595は、DVD2aに

【0150】したがって、この実施の形態9に係る記録メディア用著作権保護システム1iの復号化装置200i、すなわち、DVDドライブ400とDVD再生PCソフト500で構成されたPCであっても、HD-DVDと同様に、コンテンツを復号するための鍵を得るためには、DVD2aにバインドされた公開鍵証明書無効化リストCRLを渡さなければならなくなり、公開鍵証明書無効化リストCRLのすり替えを行うような不正なデ

【0151】なお、復号化装置200i、すなわちPCがインターネットに接続されているような場合には、DVD2eの再生の際に端末装置300にアクセスし、端末装置300から最新のCRLをダウンロードし、ダウンロードした最新のCRLを用いて、DVDドライブ400がRevokeされているか否かを公開鍵有効性検査部520で検査してもよい。

【0152】また、実施の形態9の復号化装置200iでは、DVDドライブ400と、DVD再生PCソフト500で構成したが、実際にはDVD再生PCソフトも、いわゆる「デスクランブル」機能しか有せず、ライセンス供給保護モジュールAをつないで使用する場合も想定される。すなわち、PCにICカード210aを装着できるようにし、このPCにより構成される復号化装置200iをDVDドライブ400と、ICカード210aと、Dec処理部595部分のDVD再生PCソフトとで構成してもよい。

【0153】この場合には、DVDドライブ400とICカード210aとでSACを形成し、ICカード210aと、Dec処理部595部分のDVD再生PCソフトとでSACを形成した後、DVDドライブ400により読み出された暗号化コンテンツをコンテンツ鍵で復号化し、コンテンツを再生すればよい。

【0154】また、暗号化装置100aに、さらに、復号化装置200iにおいて復号化されたコンテンツ鍵が正しいものであるか否かを確認するための基準となる確認データをDVD2aに出力する確認データ出力部を備える構成とし、この確認データ出力部は、所定の固定パ

ターンのデータをコンテンツ鍵記憶部113に記憶されたコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2fに出力する構成又は、確認データ出力部は、コンテンツ鍵をコンテンツ鍵で暗号化して得られるデータを確認データとしてDVD2fに出力する構成である場合、この端末装置110aに対応して、コンテンツ鍵復号部220iに、復号したコンテンツ鍵が正しい鍵であるか否かを判定するコンテンツ復号鍵チェック部228、コンテンツ鍵チェック部242、コンテンツ復号鍵チェック部244等を備える構成としてもよい。

【0155】以上、本発明に係る著作権保護システムについて、実施の形態に基づいて説明したが、本発明は、これらの実施の形態に限定されるものではない。例えば、上記実施の形態における著作権保護システムでは、DVDという記録媒体を介してデジタル著作物が転送されたが、インターネット等の伝送媒体を介してデジタル著作物を転送するシステムに本発明を適用することができる。つまり、記録媒体への記録に代えて伝送路への送信とし、記録媒体からの読み出しに代えて伝送路からの受信とすることで、本発明に係る著作権保護システムを適用することができる。

【0156】また、記録媒体と伝送媒体とを組み合わせでデジタル著作物を転送するシステムにも本発明を適用することができる。つまり、例えば暗号化コンテンツについてはDVDという記録媒体で提供し、暗号化コンテンツを復号化するための鍵や、CRL等については伝送媒体によるネット配信で提供してもよい。また、この逆の形、すなわち、鍵等については記録媒体で提供し、暗号化コンテンツについては伝送媒体によるネット配信で提供してもよい。この記録媒体と伝送媒体とを組み合わせでデジタル著作物を転送するシステムにおいては、暗号化コンテンツや鍵等の内、何を記録媒体で提供し、何を伝送媒体によるネット配信で提供するかは、任意に定めることができる。

【0157】また、上記実施の形態では、著作権保護モジュール（耐タンパモジュール）をICカード210a～210fで実施したが、図16に示されるように、ICカード210a～210fの各機能構成を1チップに集積化したLSI210iで構成してもよく、このLSI210iをソケット210jに装着したり、半田等で基板に直付けして装着するようにしてもよい。また、上記実施の形態では、ICカード210a～210fを著作権保護ライセンスが供給するものとして説明したが、この復号化装置200a～200fの製造メーカーが製造したICカード210a～210fやLSI210iであってもよい。

【0158】また、上記実施の形態においては、著作権保護ライセンスやコンテンツ製造メーカーの暗号化装置100a～100fとユーザが使用する復号化装置200



a～200fとの間の広域で本発明に係る著作権保護システムを適用する場合について説明したが、家庭内や一企業内等狭いエリアにおいてデジタル著作物であるコンテンツを暗号化通信する際の処理に、本著作権保護システムを適用することができる。

【0159】（実施の形態10）図17は小規模のホームLANを介してコンテンツを暗号化通信する著作権保護システムの全体構成を示すブロック図であり、図18は図17に示されるAVサーバ100j及び各プラズマTV200k、VTR200m、DVDレコーダ200nの構成を示すブロック図である。なお、図18においては、プラズマTV200k、VTR200m、DVDレコーダ200nの構成が著作権保護機構部分について同じであるので、これらの代表例としてプラズマTV200kの構成のみが図示されている。

【0160】この著作権保護システム1jは、転送媒体としてのホームLAN30と、このホームLAN30に接続されるAVサーバ100jと、クライアントとしてのプラズマTV200k、VTR200m、DVDレコーダ200nとから構成される。

【0161】AVサーバ100jは、図1に示される暗号化装置100aとほぼ同様に構成されているものの、家庭外部から受信したコンテンツをHDD等により構成されるコンテンツ記憶部161に蓄積し、プラズマTV200k、VTR200m、DVDレコーダ200nからの蓄積コンテンツ配信要求に応じて要求されたコンテンツ等をホームLAN30を介してネット配信する点が、暗号化装置100aの場合と大きく異なっている。

【0162】より詳しくは、AVサーバ100jは、放送局100gから衛星放送（BS、CS）や、地上波放送の放送網3aを介してコンテンツを受信したり、コンテンツプロバイダのサーバ100hからインターネット網3bを介してコンテンツを受信したり、CATV局100iからCATV網3cを介してコンテンツを受信したりし、受信したコンテンツをコンテンツ記憶部161に蓄積する。

【0163】そして、AVサーバ100jは、セッション鍵記憶部112aを備えており、クライアントのいずれか、例えばプラズマTV200kからコンテンツ記憶部161に蓄積している蓄積コンテンツの配信要求があった場合、この配信要求に基づいてプラズマTV200kとの間でSACを形成し、SAC形成の際に得られたセッション鍵Ksesをセッション鍵記憶部112aに格納し、暗号化装置100aで用いられていたデバイス鍵に代えてセッション鍵Ksesを用いてコンテンツ鍵Kcを暗号化する点が、デバイス鍵を用いてコンテンツ鍵Kcを暗号化する暗号化装置100aの場合と大きく異なっている。即ち、デバイス鍵に代替してセッション鍵Ksesが用いられる点が、暗号化装置100aの場合と大きく異なっている。

【0164】一方、プラズマTV200k、VTR200m、DVDレコーダ200nは、図1に示される復号化装置200aとほぼ同様に構成されているものの、AVサーバ100jとの間におけるSAC形成の際に得られたセッション鍵Ksesを記憶するためのセッション鍵記憶部221aをそれぞれ備え、セッション鍵記憶部221aに記憶されたセッション鍵Ksesを用いてコンテンツ鍵Kcを復号化する点が、デバイス鍵KD\_Aを用いてコンテンツ鍵Kcを復号化する復号化装置200aの場合と大きく異なっている。即ち、デバイス鍵KD\_Aに代替してセッション鍵Ksesが用いられる点が、復号化装置200aの場合と大きく異なっている。

【0165】次いで、この著作権保護システム1jのAVサーバ100jとプラズマTV200kとで行われる処理について、著作権保護システム1aとの相違点を中心に説明する。

【0166】AVサーバ100jは、クライアントであるDVDレコーダ200nからコンテンツ配信の要求があると、プラズマTV200kとの間で、楕円暗号を用いてSAC処理を行う。そして、同じ値のセッション鍵Ksesを相互に持ち合い、AVサーバ100jはセッション鍵記憶部112aにセッション鍵Ksesを格納し、プラズマTV200kの著作権保護モジュール210kにおけるコンテンツ鍵復号部220hは、セッション鍵記憶部221aにセッション鍵Ksesを格納する。次いで、AVサーバ100jのEx-OR部115は、プラズマTV200k間で共有されたセッション鍵Ksesと、CRLのハッシュ値とをXORする。そして、Enc部116は、Ex-OR部115によって得られた値を鍵として用いて、コンテンツ鍵Kcを暗号化する。次いで、Enc部162は、コンテンツ鍵Kcで、AVデータの要求されたコンテンツを暗号化する。コンテンツ鍵及びコンテンツの暗号化が終わると、AVサーバ100jは、CRLと共に、暗号化コンテンツ鍵及び暗号化コンテンツをホームLAN30を介してプラズマTV200kに送信する。

【0167】プラズマTV200k内の著作権保護モジュール210kは、ホームLAN30を介して送信されてきたCRL及び暗号化コンテンツ鍵を受信し、また、デスクランブラ260は、CRL及び暗号化コンテンツを受信する。次いで、プラズマTV200kの著作権保護モジュール210kにおけるコンテンツ鍵復号部220hのEx-OR部223は、セッション鍵記憶部221aに記憶されているセッション鍵Ksesと、ハッシュ関数処理部222によって得られたCRLのハッシュ値とをXORする。次いで、Dec処理部224は、Ex-OR部223によって得られた値を鍵として用いてコンテンツ鍵を復号化する。そして、プラズマTV200k内の著作権保護モジュール210kと、デスクランブラ260との間で、送られてきたCRLに基づいて、



SAC処理を行い、セッション鍵KKを共有する。

【0168】次いで、著作権保護モジュール210kの認証部237は、共有したセッション鍵KKで、コンテンツ鍵Kcを暗号化し、デスクランブラ260に送信し、デスクランブラ260の認証部277はコンテンツ鍵Kcを復号化する。Dec処理部280は、入手したコンテンツ鍵Kcにて、暗号化コンテンツを復号化する。したがって、家庭や企業等比較的小さなネットワークに接続されたクライアントにおいても容易にコンテンツ利用ができ、しかも、末端のクライアントまで著作権保護を徹底化することができる。

【0169】なお、本実施の形態10においては、デバイス鍵に代えてセッション鍵Ksesを用いたが、AVサーバ100jとプラズマTV200k間で、秘密鍵Ksを予め共有しているものとしてもよい。この場合には、セッション鍵Ksesに代えて秘密鍵Ksを用いればよい。また、復号化したコンテンツ鍵が正しい値かどうかを予め調べるために、上記した固定パターンをCRL等と共に送信し、著作権保護モジュール210kにおいて予め確認できるように構成してもよい。

【0170】また、本発明は、上記10個の実施の形態における特徴的な処理を組み合わせることで、様々な暗号化装置や復号化装置を実現することができる。つまり、暗号化の場合であれば、(1)秘密鍵に対する暗号化やメディアIDに対する一方向関数による変換それぞれを層と呼んだ場合に、その層の数に関しては、2層にするか、3層にするかの選択が可能であり、(2)コンテンツの暗号化に用いる鍵に関しては、コンテンツ鍵にするか、メディアIDを一方向性関数で変換して得られる関数値にするかの選択が可能であり、(3)公開鍵無効化リストのハッシュ値を関与させる対象に関しては、デバイス鍵にするか、ディスク鍵にするか、コンテンツ鍵にするか、メディアIDにするか、セッション鍵にするか、メディアIDを一方向性関数で変換して得られる関数値にするかの選択が可能である。

【0171】したがって、それらの独立したパラメータ(1)、(2)、(3)それぞれの1つずつを任意に組み合わせることで、様々な形態の暗号化装置、復号化装置及びICカードを実現することができる。また、上記秘密鍵等の暗号化(又は、復号化)の層数としては1～3に限定されるものではなく、3層を超えるものであってもよい。これらのバリエーションを考慮して本発明の暗号化装置、復号化装置及びICモジュール(秘密鍵生成装置)を表現すると以下のように言うことができる。

【0172】つまり、コンテンツ鍵を使用する暗号化方法であれば、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、 $n$  ( $\geq 2$ ) 個の秘密鍵のうち、第1秘密鍵を用いてデジタル著作物を暗号化するとともに、第 $i$  ( $2 \leq i \leq n$ ) 秘密鍵を用いて第 $(i-1)$ 秘密鍵を暗号化するという暗号化の連鎖

を前記第1～第 $(n-1)$ 秘密鍵について繰り返し、暗号化された第1～第 $(n-1)$ 秘密鍵を前記媒体に出力する方法であって、前記第1～第 $n$ 秘密鍵の少なくとも1つを用いた暗号化においては、その暗号化に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくことを特徴とする暗号化方法である。

【0173】また、メディアIDを使用する暗号化方法であれば、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置において、 $n$  ( $\geq 1$ ) 個の秘密鍵のうち、第1秘密鍵を用いて媒体識別情報を一方向性関数で変換した後に、変換された媒体識別情報でデジタル著作物を暗号化するとともに、前記 $n$ が2以上の場合に、第 $i$  ( $2 \leq i \leq n$ ) 秘密鍵を用いて第 $(i-1)$ 秘密鍵を暗号化するという暗号化の連鎖を前記第1～第 $(n-1)$ 秘密鍵について繰り返し、暗号化された第1～第 $(n-1)$ 秘密鍵を前記媒体に出力する方法であって、前記第1～第 $n$ 秘密鍵の少なくとも1つを用いた暗号化又は変換においては、(1)その暗号化又は変換に先立ち、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストの内容に依存する属性値を用いて秘密鍵を変形させておくか、又は、(2)前記変換によって得られた媒体識別情報を前記属性値で変形させておくことを特徴とする暗号化方法である。また、コンテンツ鍵を使用する復号化方法であれば、暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と $n$  ( $\geq 2$ ) 個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記 $n$ 個の暗号化秘密鍵のうちの第1暗号化秘密鍵を復号化し、得られた第1秘密鍵で第2暗号化秘密鍵を復号化するという復号化の連鎖を前記 $n$ 個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第 $n$ 秘密鍵でデジタル著作物を復号化する方法であって、前記第1～第 $n$ 暗号化秘密鍵に対する復号化の少なくとも1つにおいては、その復号化に先立ち、復号化に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくことを特徴とする復号化方法である。

【0174】また、メディアIDを使用する復号化方法であれば、暗号化されたデジタル著作物を復号化する復号化装置において、暗号化されたデジタル著作物と媒体識別情報と $n$  ( $\geq 1$ ) 個の暗号化秘密鍵と無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストとを記録媒体又は伝送媒体を介して取得した後に、予め保持している秘密鍵を用いて前記 $n$ 個の暗号化秘密鍵のうちの第1暗号化秘密鍵を復号化し、前記 $n$ が2以上の場合に、前記復号化で得られた第1秘密鍵で第2暗号化秘密鍵を復号化するという復号化の連鎖を前記



n個の暗号化秘密鍵について繰り返し、最後の復号化で得られた第n秘密鍵を用いて前記媒体識別情報を一方向性関数で変換し、変換後の媒体識別情報をデジタル著作物を復号化する方法であって、前記第1～第n暗号化秘密鍵に対する復号化及び前記媒体識別情報に対する変換の少なくとも1つにおいては、(1)その復号化又は変換に先立ち、復号化又は変換に用いる秘密鍵を前記公開鍵無効化リストの内容に依存する属性値で変形させておくか、又は、(2)前記変換によって得られた媒体識別情報を前記属性値で変形させておくことを特徴とする復号化方法である。

【0175】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号化装置は、デジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第2秘密鍵記憶手段に記憶された第2秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記変形手段により変形された第2秘密鍵で暗号化する第1暗号化手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化する第2暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。

【0176】これによって、暗号化装置からは、暗号化されたデジタル著作物と、その暗号化に用いられた第1秘密鍵の暗号化されたもの(暗号化第1秘密鍵)と、公開鍵無効化リストとが出力されるが、その暗号化第1秘密鍵は、復号化装置に対応づけられた第2秘密鍵によって単に第1秘密鍵が暗号化されているのではなく、公開鍵無効化リストが関与した第2秘密鍵によって暗号化されている。したがって、これら暗号化デジタル著作物、暗号化第1秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストが差し替えられていた場合には、内部に有する第2秘密鍵に対する公開鍵無効化リストによる関与の内容が異なったものとなり、そのように変形された第2秘密鍵を用いて暗号化第1秘

秘密鍵を本来の第1秘密鍵に復号化することができず、したがって、暗号化デジタル著作物を正しく復号化することができない。よって、公開鍵無効化リストの差し替え攻撃に対する防御機能を有した安全なデジタル著作物の転送が可能となる。

【0177】ここで、前記暗号化装置は、さらに、前記復号化装置において復号化された第1秘密鍵が正しいものであるか否かを確認するための基準となる確認データを前記記録媒体又は伝送媒体に出力する確認データ出力手段を備えてもよい。例えば、前記確認データ出力手段は、所定の固定パターンのデータを前記第1秘密鍵記憶手段に記憶された第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力したり、前記確認データ出力手段は、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を当該第1秘密鍵で暗号化して得られるデータを前記確認データとして前記記録媒体又は伝送媒体に出力してもよい。

【0178】これによって、この暗号化装置から出力された暗号化デジタル著作物、暗号化第1秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストの差し替え攻撃を受けたか否か、つまり、正しい第1秘密鍵に復元することができたか否かを判断することができるので、誤った第1秘密鍵でデジタル著作物を復号化するという無駄な処理を事前に回避することが可能となる。

【0179】また、本発明に係る暗号化装置は、デジタル著作物であるデジタル著作物を暗号化し、記録媒体又は伝送媒体に出力する暗号化装置であって、デジタル著作物を記憶するデジタル著作物記憶手段と、デジタル著作物の暗号化に用いられる第1秘密鍵を記憶する第1秘密鍵記憶手段と、暗号化されたデジタル著作物を復号する復号化装置に対応づけられた第2秘密鍵を記憶する第2秘密鍵記憶手段と、無効化された公開鍵証明書を特定する情報の一覧である公開鍵無効化リストを記憶する公開鍵無効化リスト記憶手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記第2秘密鍵記憶手段に記憶された第2秘密鍵で暗号化する第1暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リストに基づいて、その公開鍵無効化リストの内容に依存する属性値を算出する属性値算出手段と、前記第1秘密鍵記憶手段に記憶された第1秘密鍵を前記属性値算出手段により算出された属性値で変形させる変形手段と、前記デジタル著作物記憶手段に記憶されたデジタル著作物を前記変形手段により変形された第1秘密鍵で暗号化する第2暗号化手段と、前記公開鍵無効化リスト記憶手段に記憶された公開鍵無効化リスト、前記第1暗号化手段により暗号化された第1秘密鍵および前記第2暗号化手段により暗号化されたデジタル著作物を記録媒体又は伝送媒体に出力する出力手段とを備えることを特徴とする。



【0180】これによって、暗号化装置からは、暗号化されたデジタル著作物と、その暗号化に用いられた第1秘密鍵の暗号化されたもの（暗号化第1秘密鍵）と、公開鍵無効化リストとが出力されるが、その暗号化デジタル著作物は、単に第1秘密鍵で暗号化されているのではなく、第1秘密鍵に公開鍵無効化リストを関与させた変形後の第1秘密鍵で暗号化されている。したがって、これら暗号化デジタル著作物、暗号化第1秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストが差し替えられていた場合には、復号化した第1秘密鍵に対する公開鍵無効化リストによる関与の内容が異なったものとなり、そのように変形された第1秘密鍵を用いて暗号化デジタル著作物を正しく復号化することができない。よって、公開鍵無効化リストの差し替え攻撃に対する防御機能を有した安全なデジタル著作物の転送が可能となる。

【0181】また、上述と同様に、第1秘密鍵に公開鍵無効化リストを関与させたものに関する確認データを添付して暗号化装置から出力することで、この暗号化装置から出力された暗号化デジタル著作物、暗号化第1秘密鍵および公開鍵無効化リストを受け取った復号化装置は、公開鍵無効化リストの差し替え攻撃を受けたか否か、つまり、デジタル著作物の暗号化に用いられた正しい秘密鍵に復元することができたか否かを判断することができるので、誤った秘密鍵でデジタル著作物を復号化するという無駄な処理を事前に回避することが可能となる。

【0182】また、本発明に係る暗号通信装置は、相手装置の公開鍵を用いて相手装置と暗号通信する装置であって、無効化された公開鍵証明書を持定する情報の一覧である公開鍵無効化リストを記憶する記憶手段と、新たな公開鍵無効化リストを取得する取得手段と、取得された公開鍵無効化リストのサイズと前記記憶手段に記憶されている公開鍵無効化リストのサイズとを比較し、取得された公開鍵無効化リストのサイズが大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段と、前記記憶手段に格納された公開鍵無効化リストを参照して相手装置の公開鍵の有効性を判断し、有効と判断した場合に、その公開鍵を用いて相手装置と暗号通信する通信手段とを備えることを特徴とする。同様に、上記格納手段に代えて、取得された公開鍵無効化リストに示された前記証明書の数と前記記憶手段に記憶されている公開鍵無効化リストに示された前記証明書の数とを比較し、取得された公開鍵無効化リストに示された前記証明書の数が大きい場合に、取得された公開鍵無効化リストを前記記憶手段に格納して更新する格納手段とすることもできる。

【0183】これによって、公開鍵証明書無効化リストに登録されている公開鍵証明書の件数は、時の経過とともに増加する一方であるので、暗号通信装置は、よりサ

イズの大きい（あるいは、より登録件数の多い）公開鍵証明書無効化リスト、すなわち、より最新の公開鍵証明書無効化リストを常に保持することが可能となる。

【0184】以上のように、本発明により、公開鍵証明書無効化リストの差し替えという攻撃に対しても安全にデジタル著作物を転送することが可能となり、インターネット等の伝送路やDVD等の記録媒体を介したデジタル著作物の配信や流通が活発になってきた今日において、その実用的価値は極めて高い。

# 10 【図面の簡単な説明】

【図1】本実施の形態1に係る記録メディア用著作権保護システムの全体構成を示す機能ブロック図である。

【図2】公開鍵証明書無効化リストCRLの構成例を示す図である。

【図3】著作権保護ライセンサ用公開鍵証明書の構成例を示す図である。

【図4】プレーヤメーカ用公開鍵証明書の構成例を示す図である。

20 【図5】復号化装置200aのICカード210aおよびデスクランブラ260間で行われる処理のシーケンスを示す図である。

【図6】本実施の形態2に係る記録メディア用著作権保護システム1bの全体構成を示す機能ブロック図である。

【図7】本実施の形態3に係る記録メディア用著作権保護システム1cの全体構成を示す機能ブロック図である。

30 【図8】本実施の形態4に係る記録メディア用著作権保護システム1dの全体構成を示す機能ブロック図である。

【図9】本実施の形態5に係る記録メディア用著作権保護システム1eの全体構成を示す機能ブロック図である。

【図10】本実施の形態6に係る記録メディア用著作権保護システム1fの全体構成を示す機能ブロック図である。

40 【図11】図11(a)は、図10の最新版検出処理部2391により行われる確認判断処理のフローチャートであり、図11(b)は、最新版リスト読み出し処理のフローチャートである。

【図12】上記実施の形態1～2に係る記録媒体用の復号化装置200a～200fをHD-DVDプレーヤに適用した場合の外観図である。

【図13】本実施の形態7に係る記録メディア用著作権保護システム1gの全体構成を示す機能ブロック図である。

【図14】本実施の形態8に係る記録メディア用著作権保護システム1hの全体構成を示す機能ブロック図である。

50 【図15】本実施の形態9に係る記録メディア用著作権



保護システム1 iの全体構成を示す機能ブロック図である。

【図16】著作権保護モジュールをLSIで構成した場合の実装例を示す図である。

【図17】小規模のホームLANを介してコンテンツを暗号化通信する著作権保護システムの全体構成を示すブロック図である。

【図18】図17に示されるAVサーバ100 j及びプラズマTV200 kの構成を示すブロック図である。

【符号の説明】

1 a ~ 1 j	著作権保護システム
2 a ~ 2 f	DVD
3 0	ホームLAN
1 0 0 a ~ 1 0 0 f	暗号化装置
1 0 0 j	AVサーバ
1 1 0 a ~ 1 1 0 f, 1 6 0, 3 0 0	
端末装置	
1 1 1	公開鍵無効化リスト
記憶部	
1 1 2	デバイス鍵束記憶部
1 1 3	コンテンツ鍵記憶部
1 1 4, 2 2 2	ハッシュ関数処理部
1 1 5, 1 1 8, 2 2 3, 2 2 6	Ex-OR部
1 1 6, 1 1 7, 1 3 1, 1 4 2, 1 4 3, 1 6 2, 2 4 1	Enc部
1 1 9	固定パターン記憶部
1 4 4	メディアID記憶部
1 4 5, 2 4 7	一方向関数部
1 6 1	コンテンツ記憶部

【図2】

CRL		
ファイルヘッダ	名前	〇△□△.cr1
	サイズ	79KB
	種類	証明書無効リスト
	更新日	2001/09/07/12:34
全般	バージョン	V1
	発行者	〇△□△
	有効開始日	2001年09月06日
	次の更新予定日	2001年09月16日
	署名のアルゴリズム	md5RSA
無効リスト	シリアル番号	無効日
	〇××…△□	2001年05月01日
	〇××…〇□	2000年11月29日
	⋮	⋮

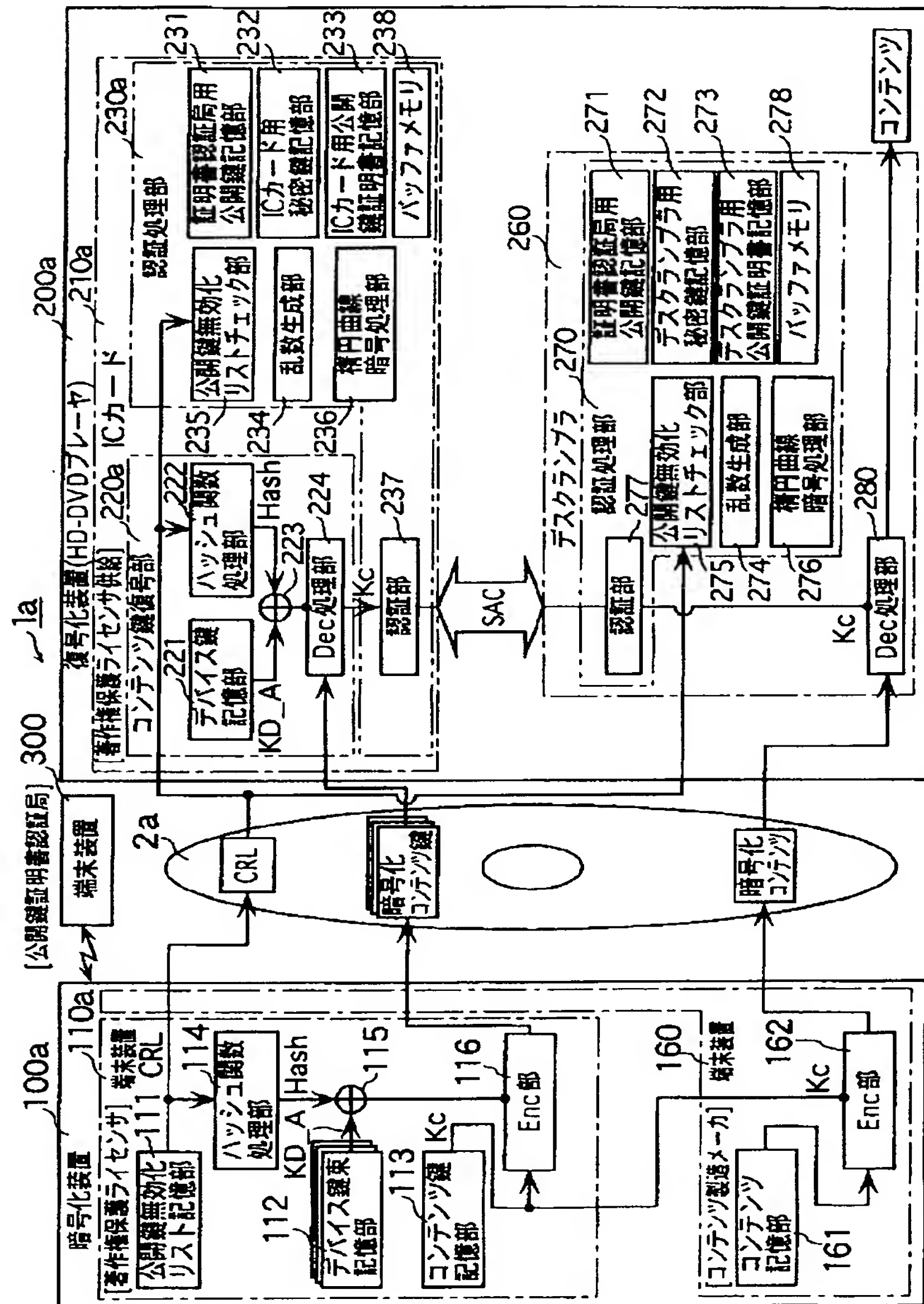
2 0 0	HD-DVDプレーヤ
2 0 0 a ~ 2 0 0 i	復号化装置
2 1 0 a ~ 2 1 0 h	ICカード
2 1 0	LSI
2 1 0 k	著作権保護モジュール
2 2 0 a ~ 2 2 0 i	コンテンツ鍵復号部
2 2 1	デバイス鍵記憶部
2 2 2	ハッシュ関数処理部
2 2 4, 2 2 5, 2 2 7, 2 4 3, 2 8 0	
Dec処理部	
2 2 8, 2 4 4	コンテンツ復号鍵チェック部
2 4 2	コンテンツ鍵チェック部
2 3 0, 2 7 0	認証処理部
2 3 9	公開鍵無効化リスト
最新版記憶処理部	
2 3 9 1	最新版検出処理部
2 3 9 2	最新版検出情報記憶部
2 3 9 3	記憶部
2 5 0	公開鍵証明書無効化リスト
最新版記憶部	
2 6 0	デスクランブラ
4 0 0	DVDドライブ
5 0 0	DVD再生PCソフト

【図3】

233
ICカード用公開鍵証明書Cert_A
ICカード210のID
ICカード用公開鍵PK_A
ICカード用公開鍵PK_Aに対する証明書認証局CAの署名
有効期限
⋮

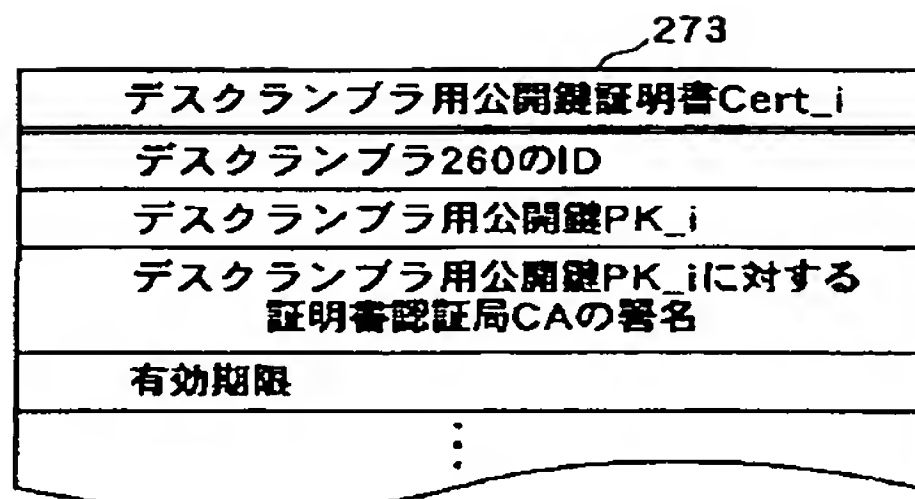


【図1】

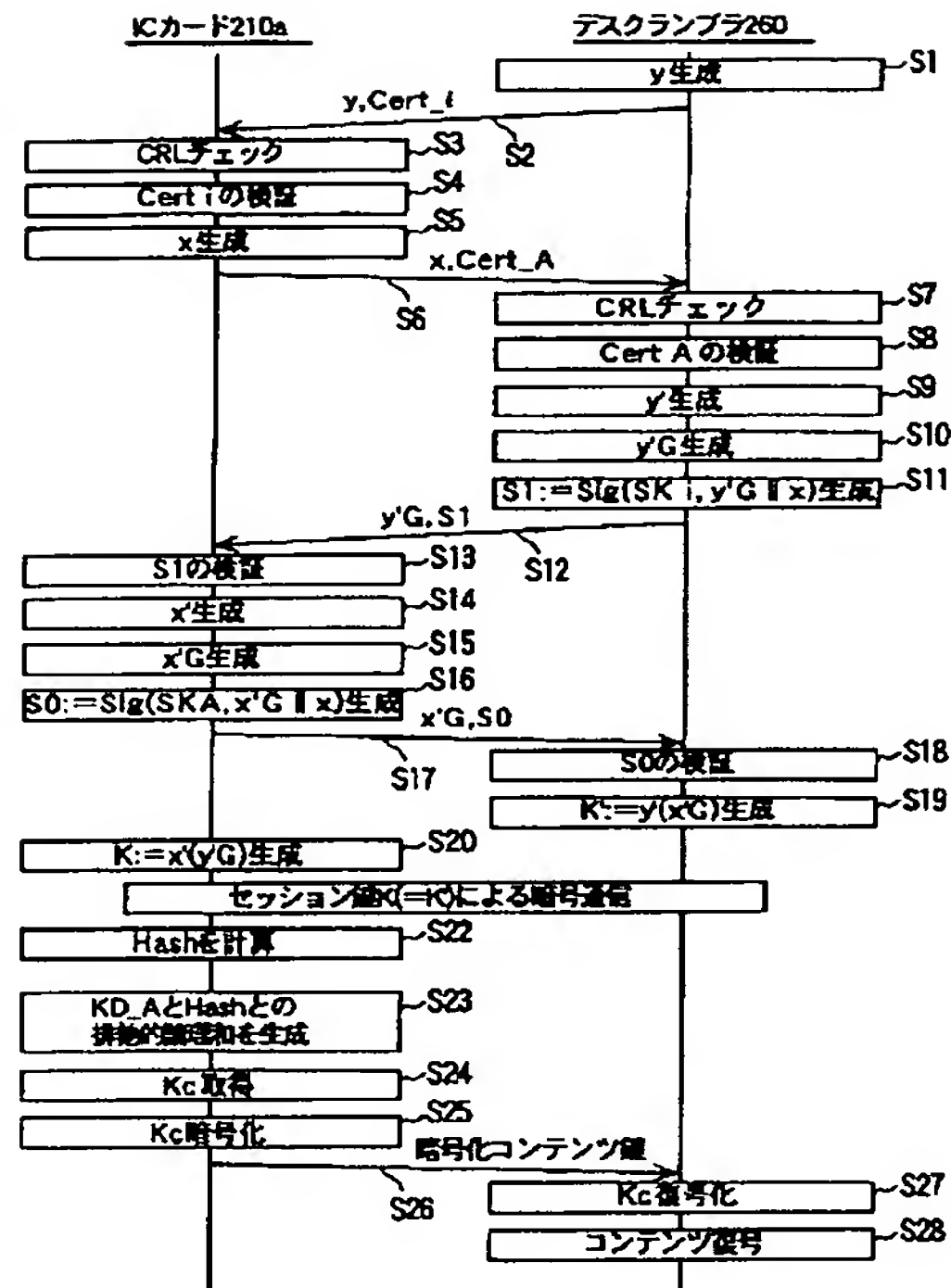




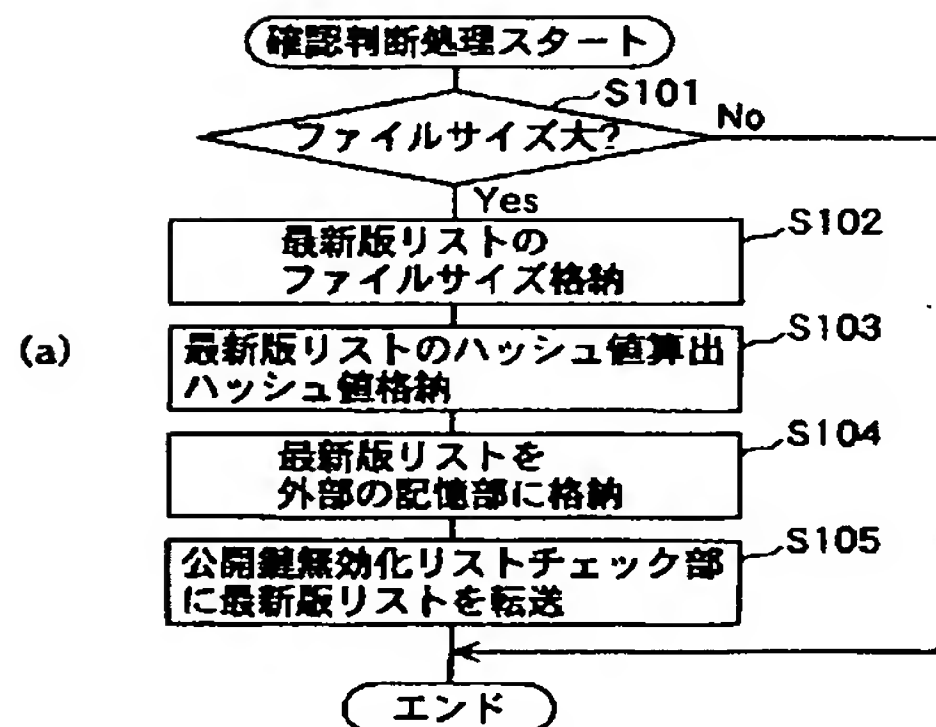
【図4】



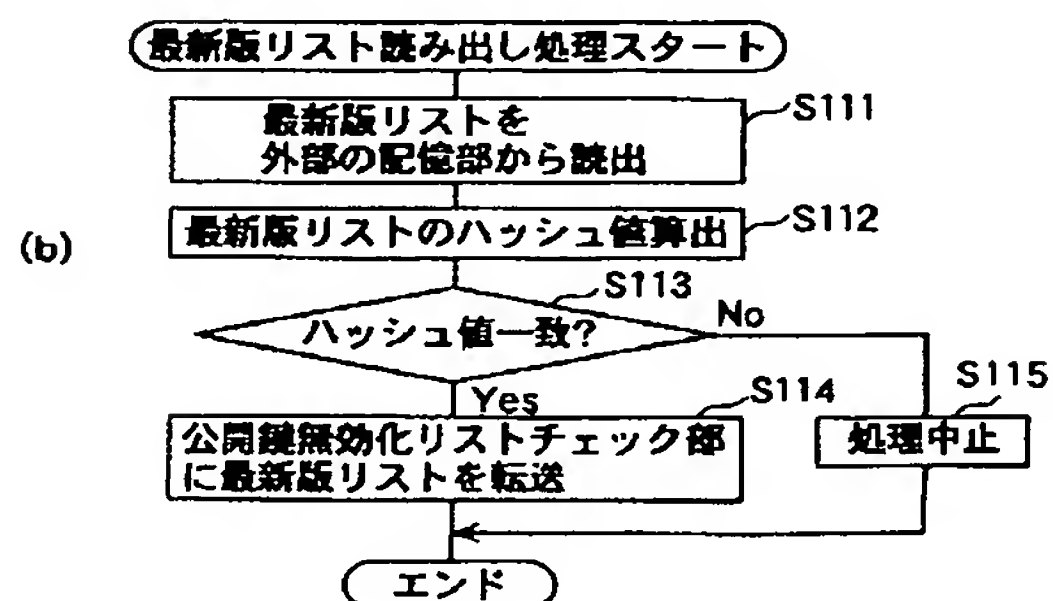
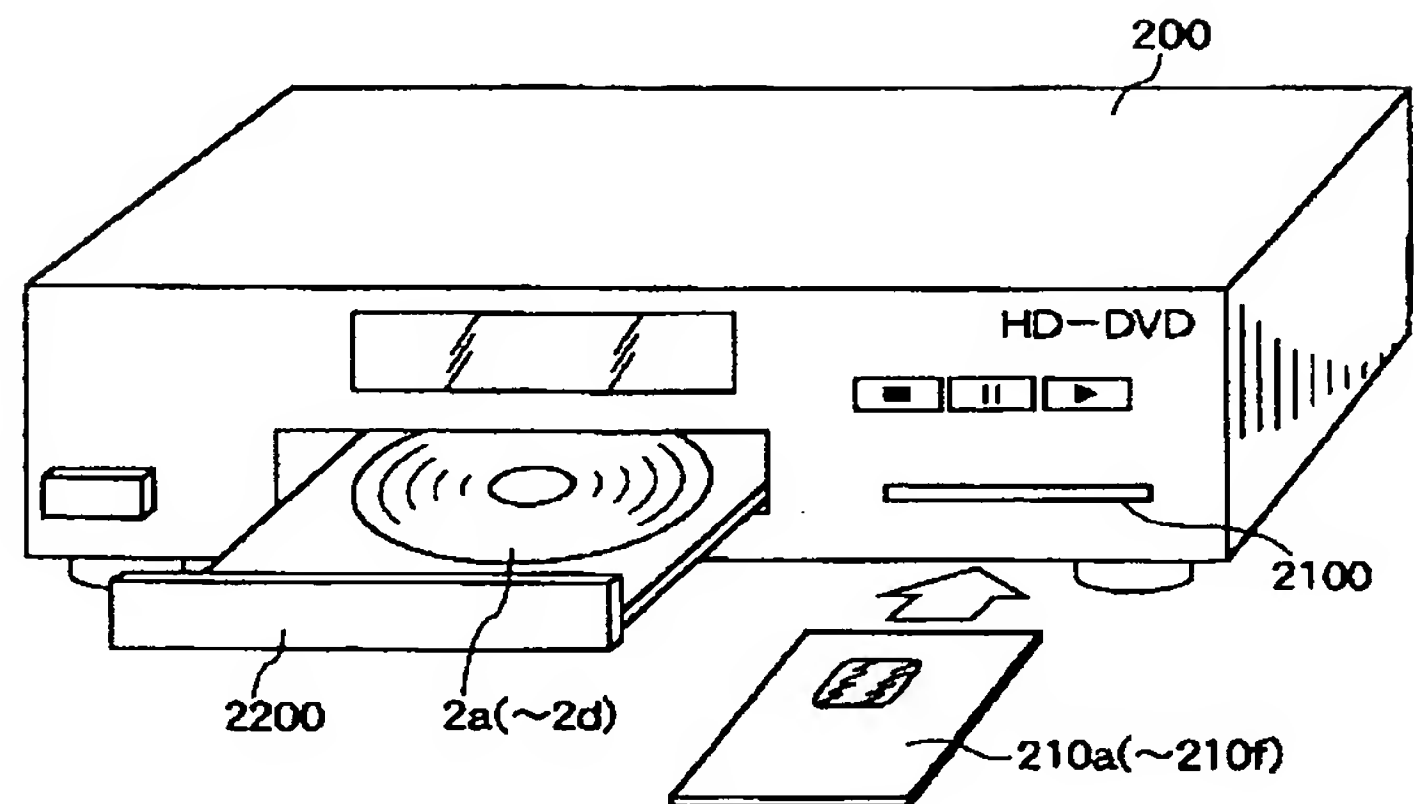
【図5】



【図11】

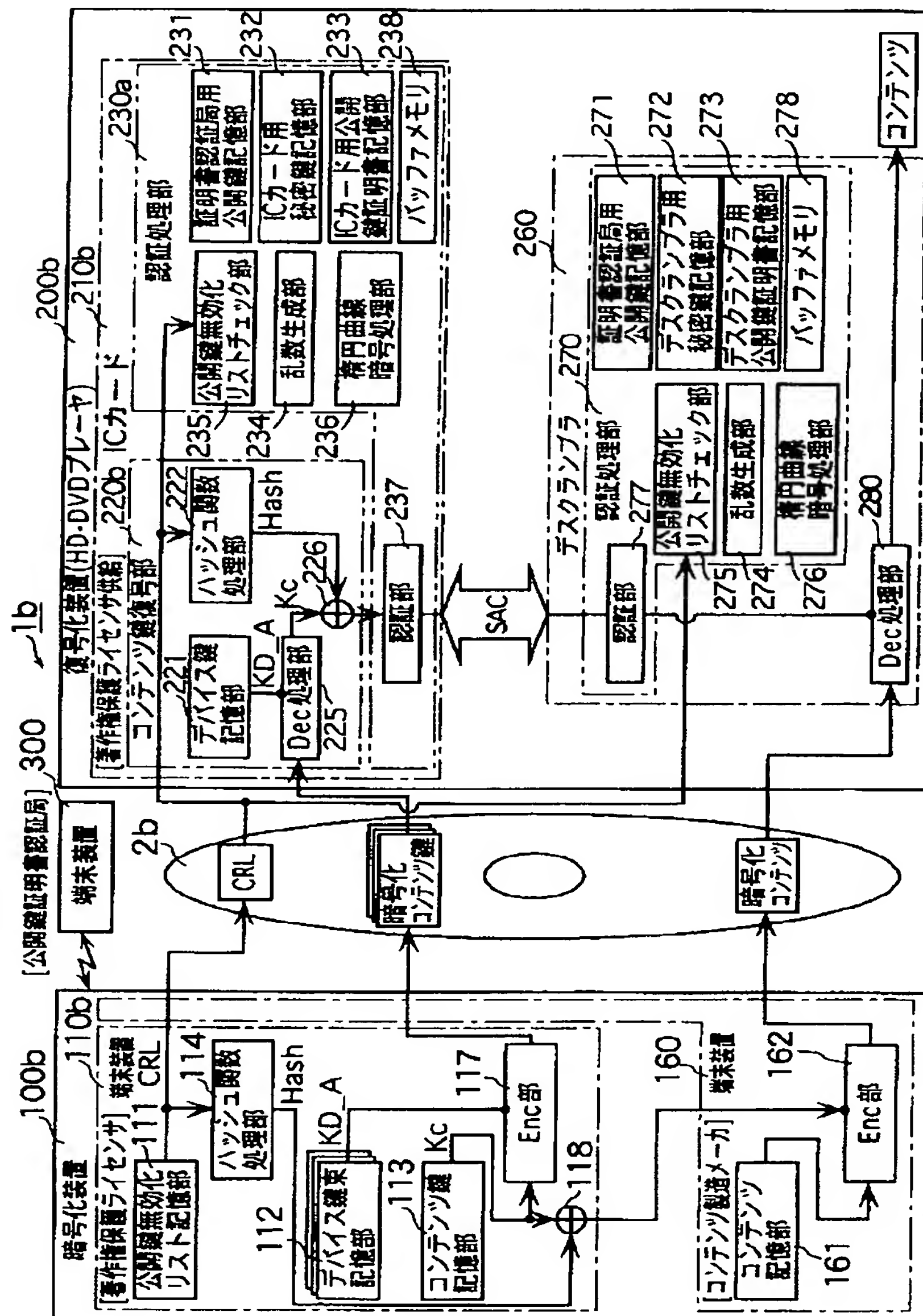


【図12】



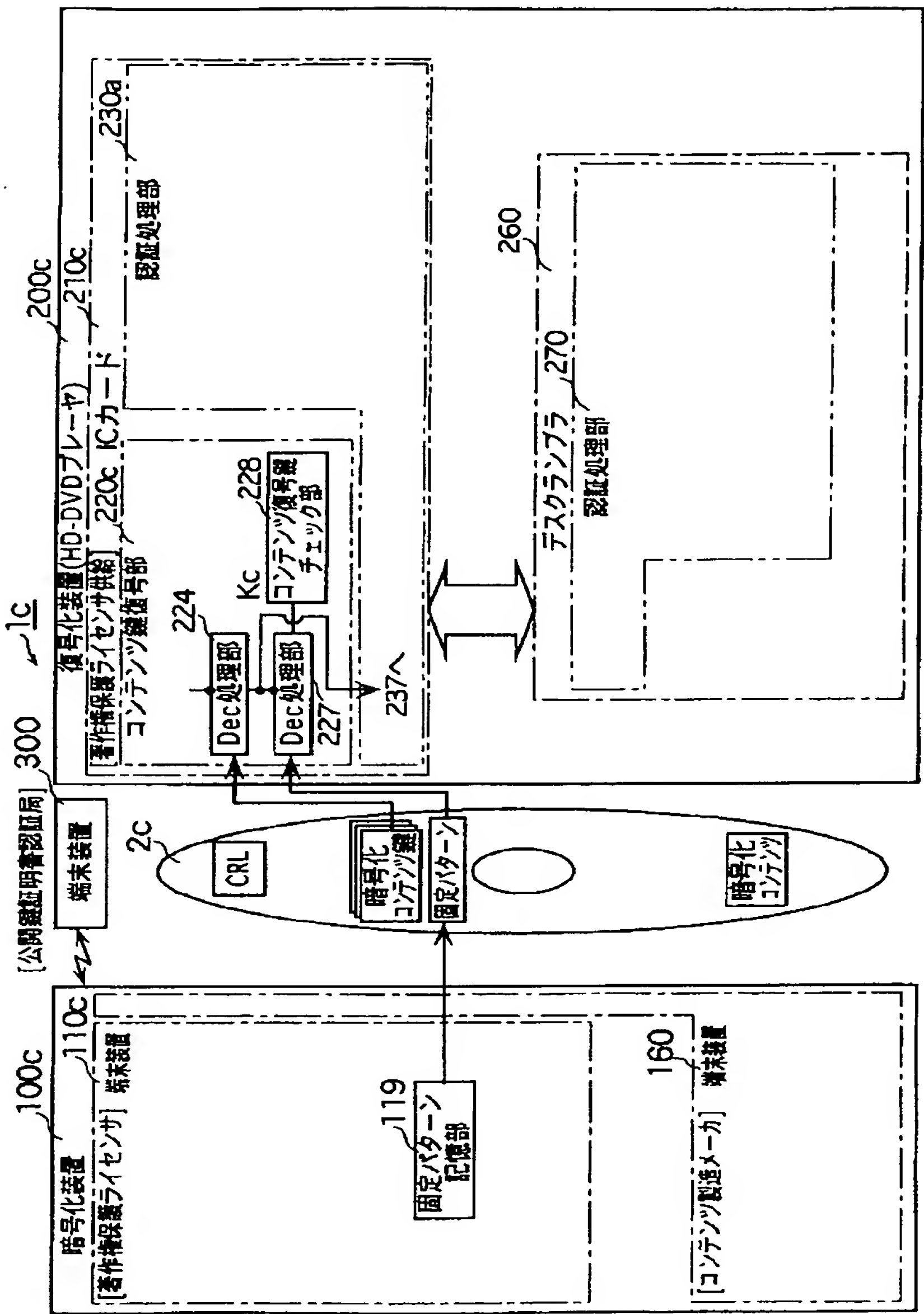


【図6】



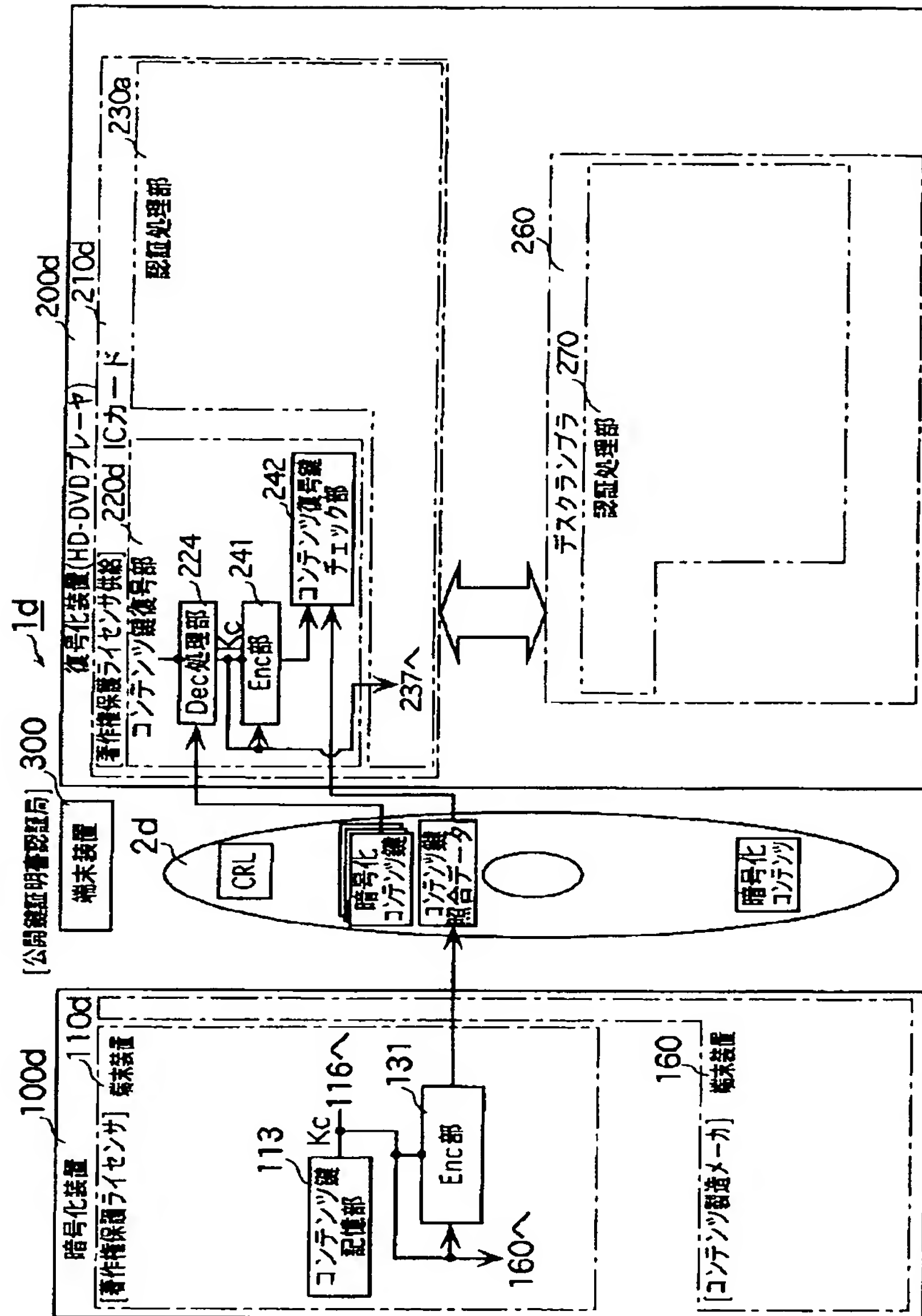


【図7】



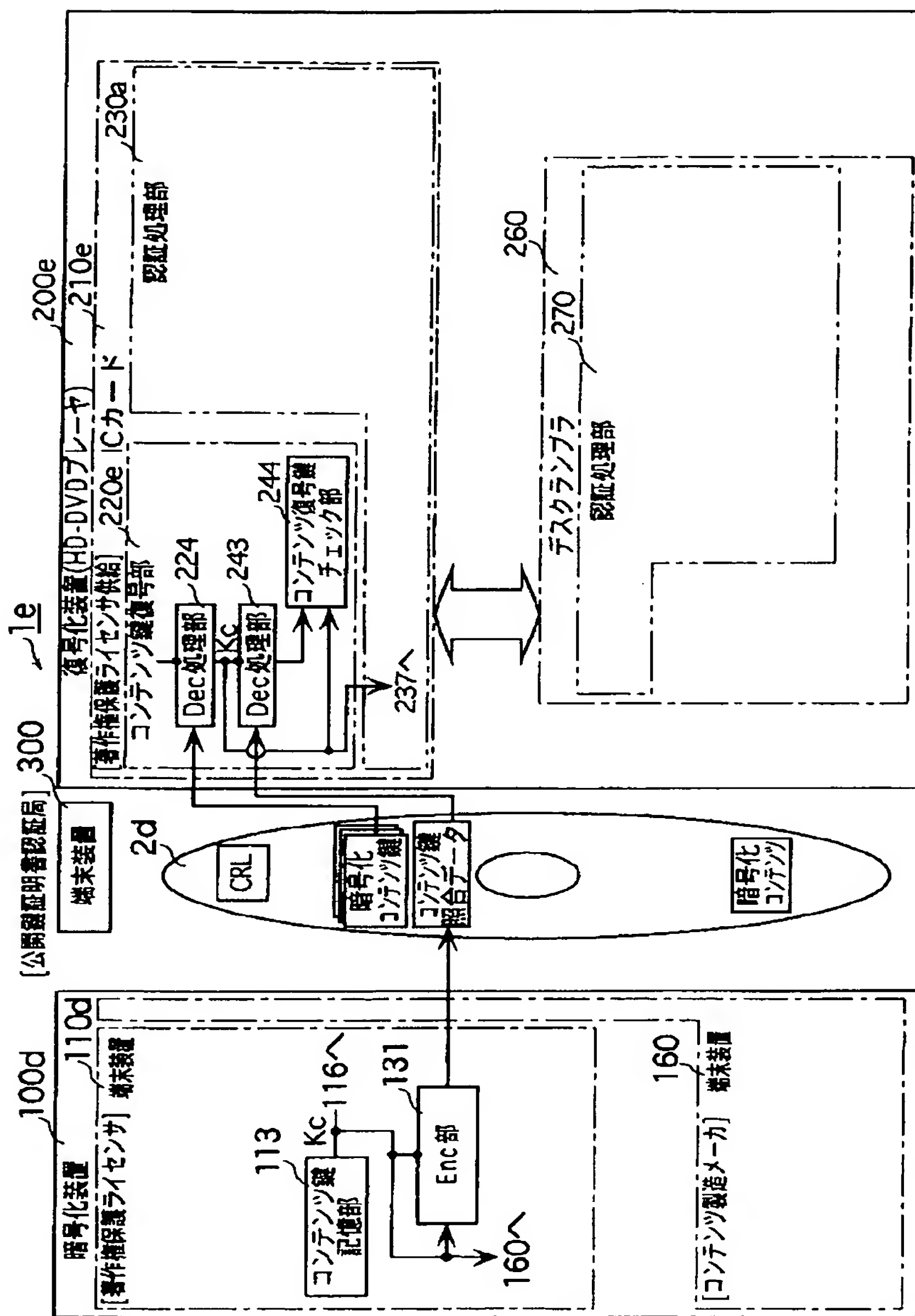


【図8】



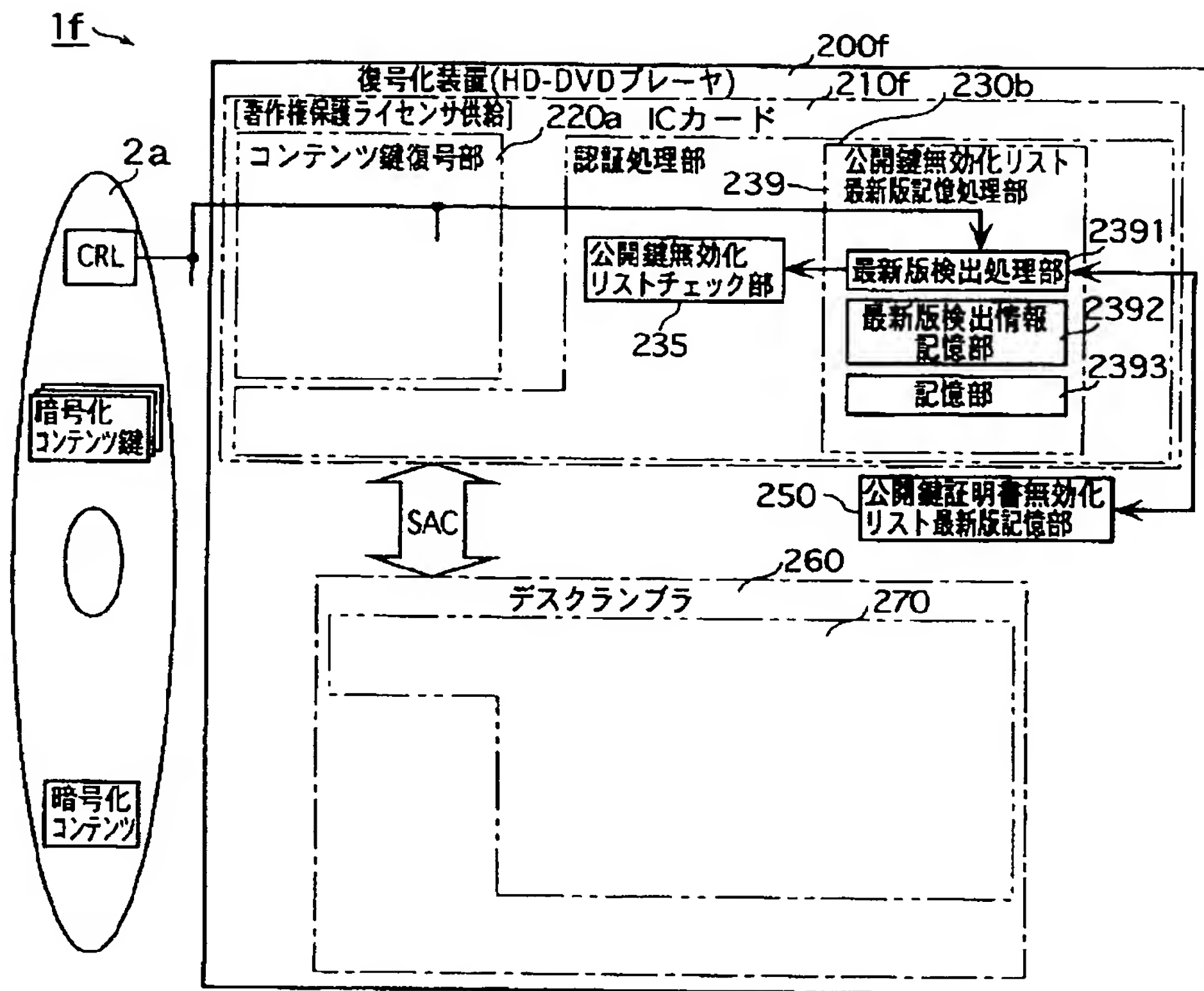


【図9】

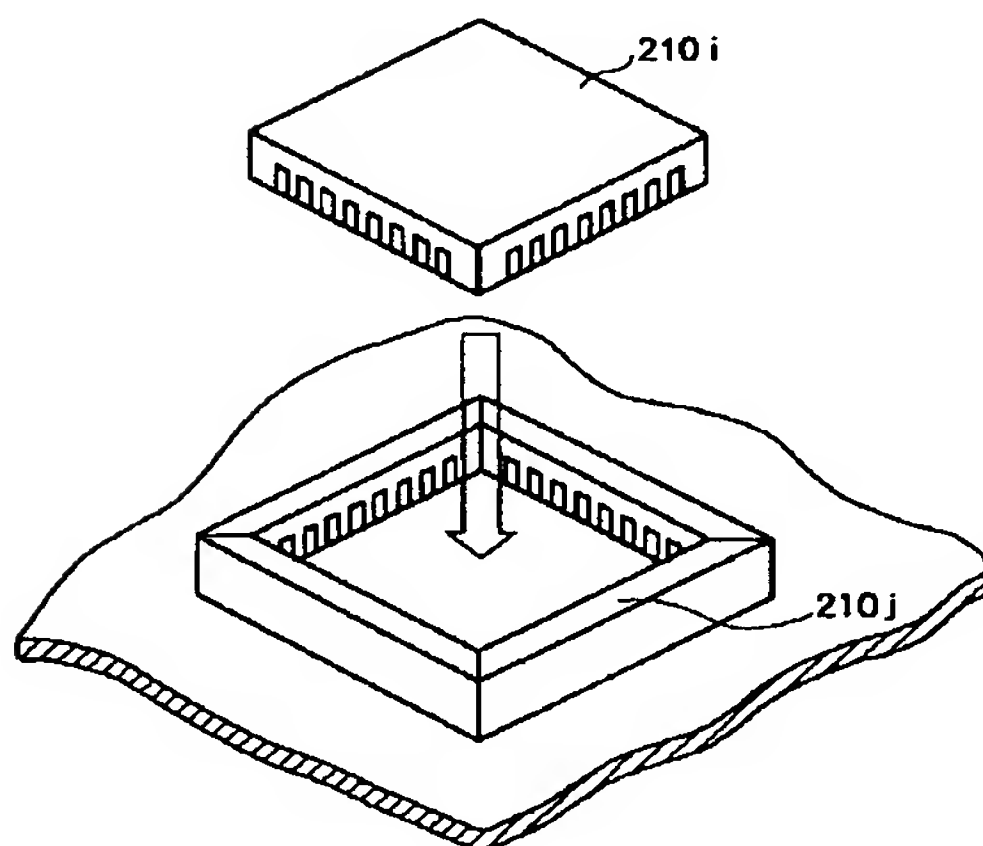




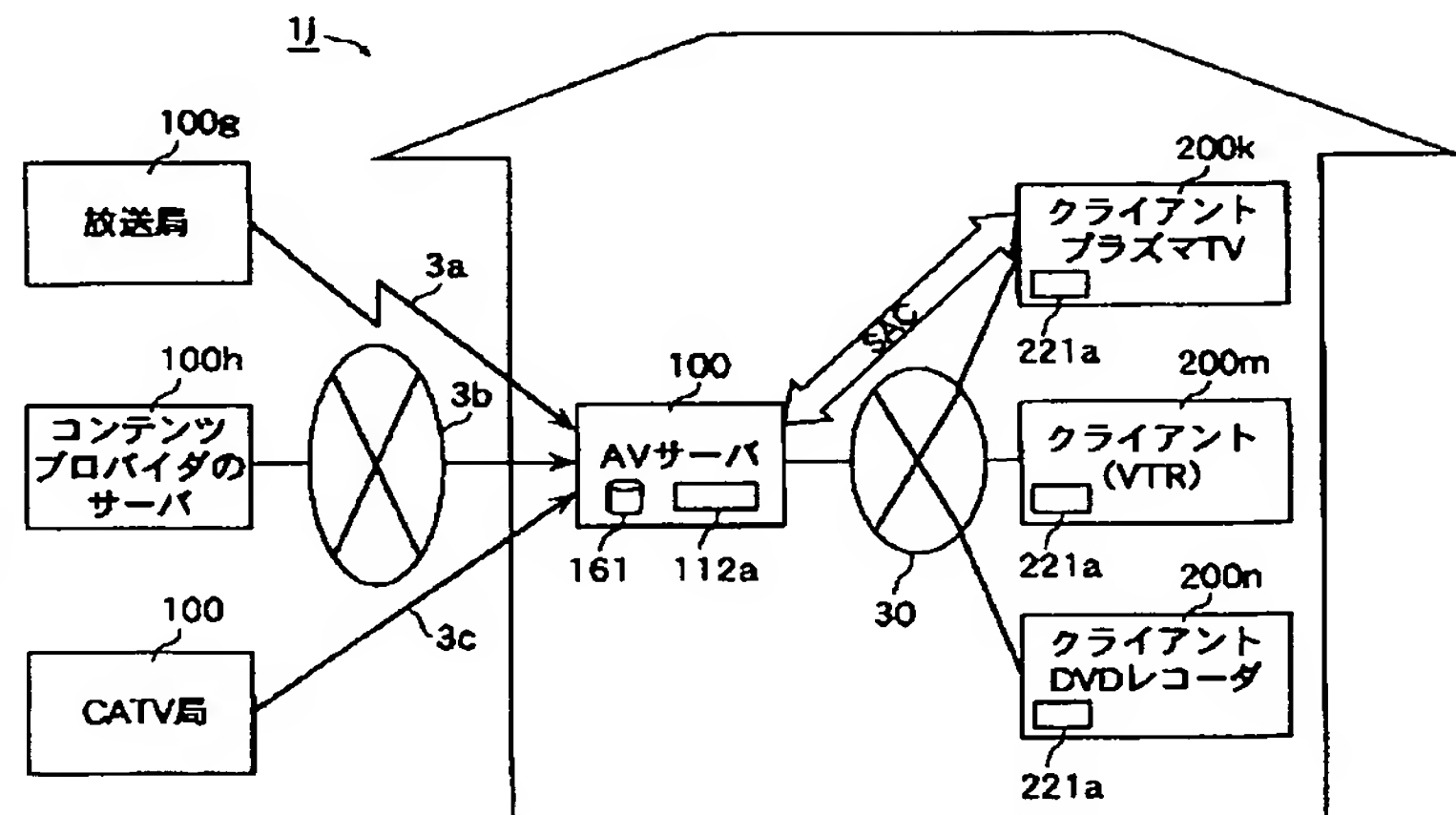
【図10】



【図16】

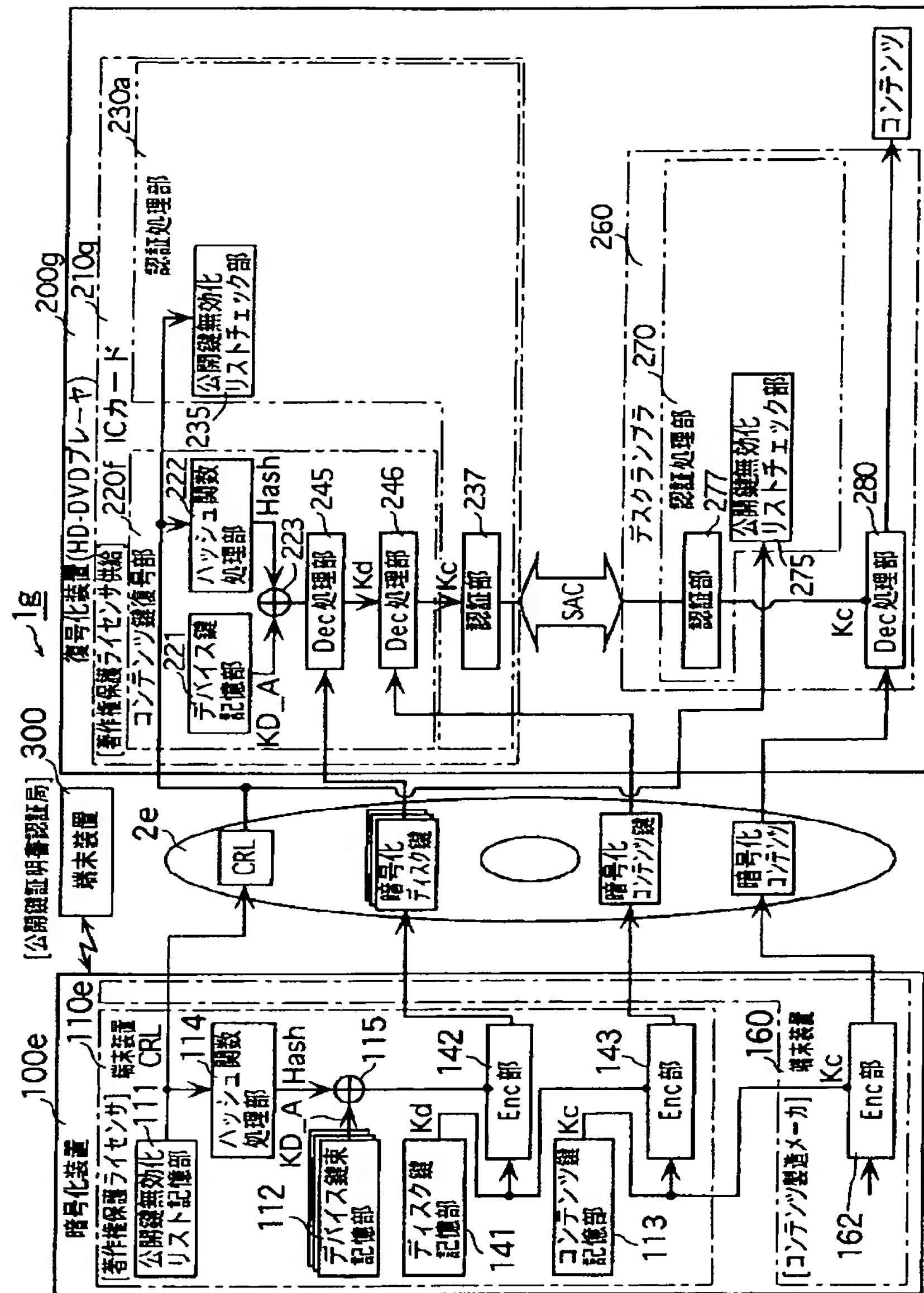


【図17】



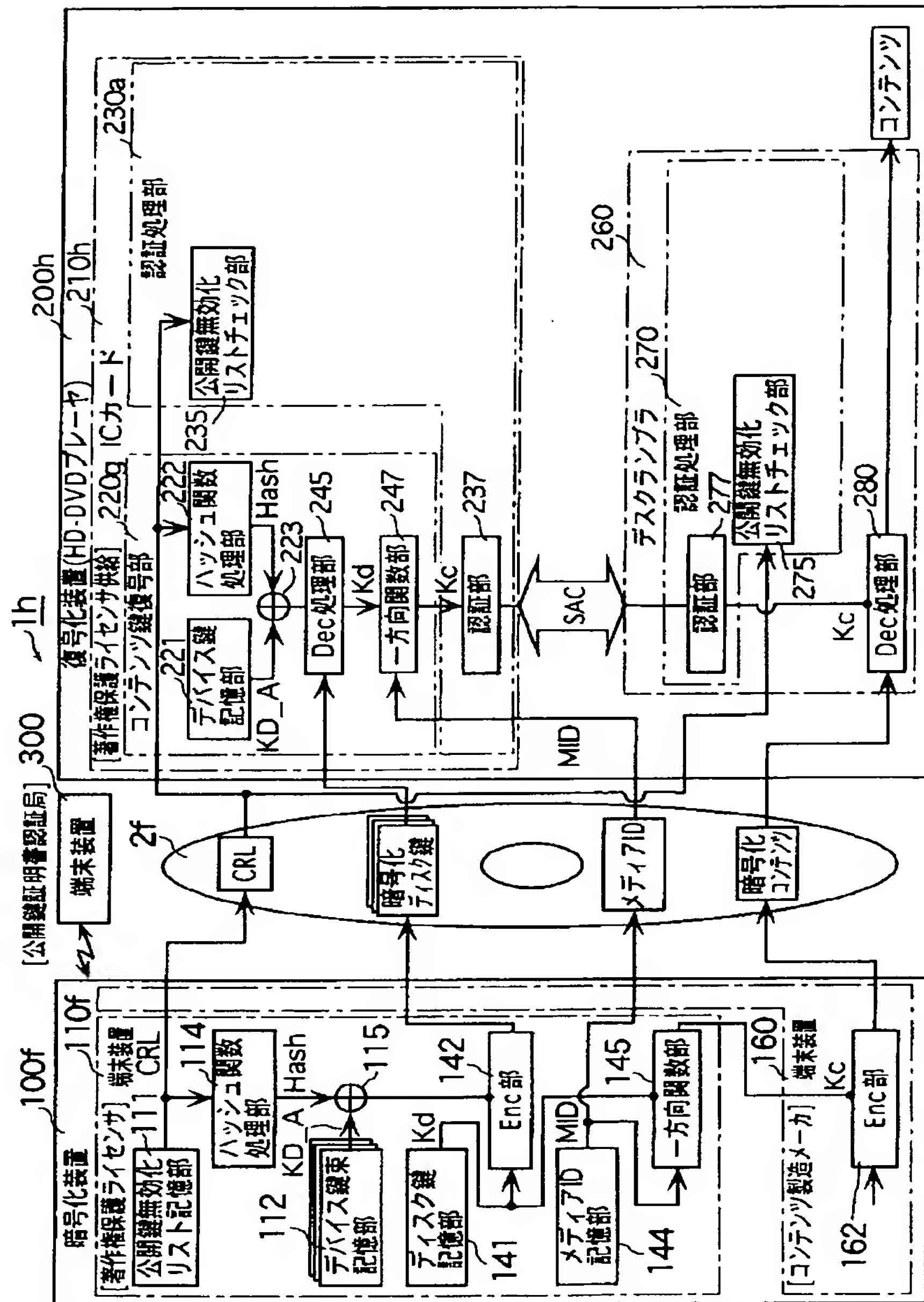


【図13】



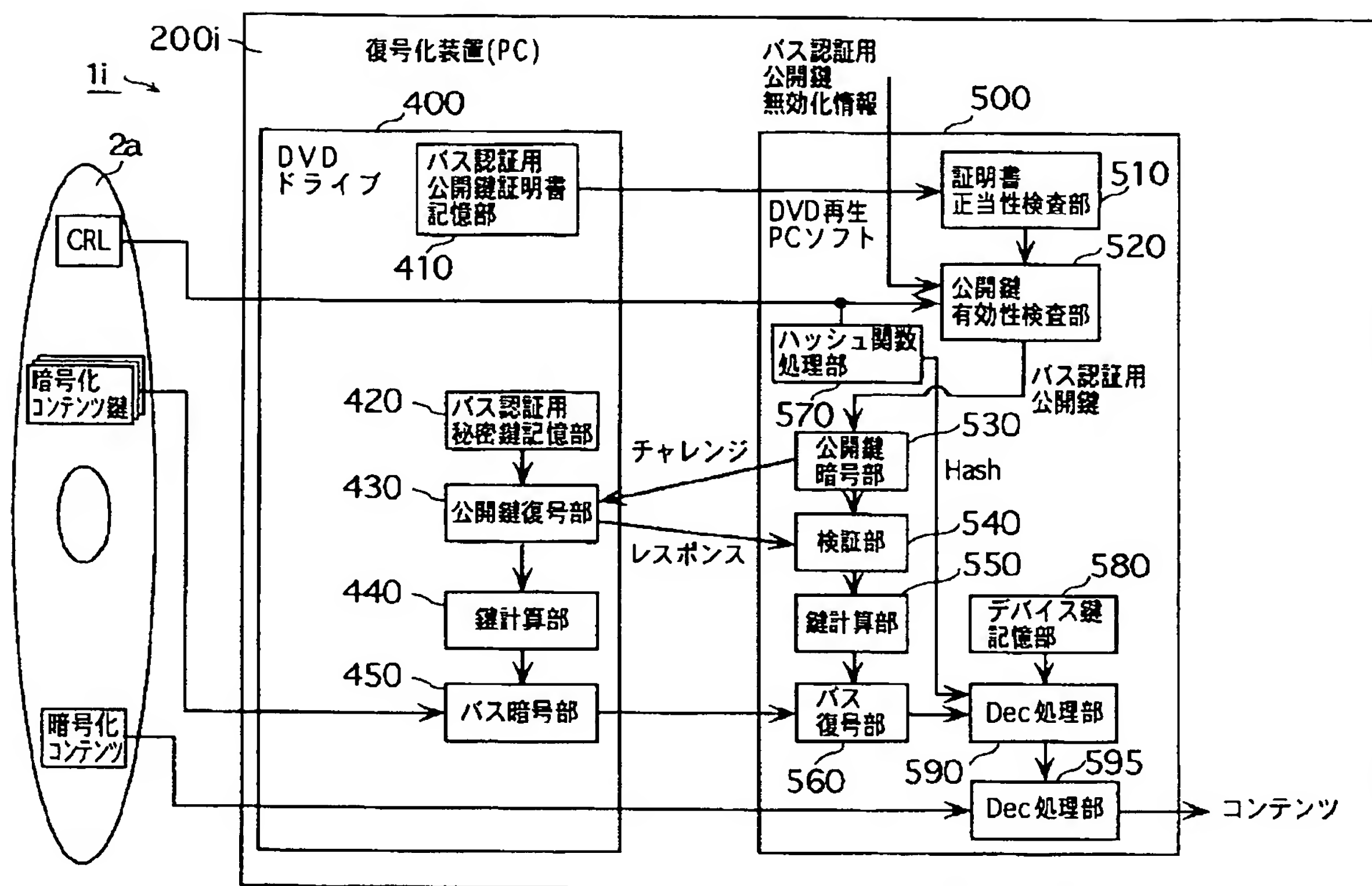


【図14】



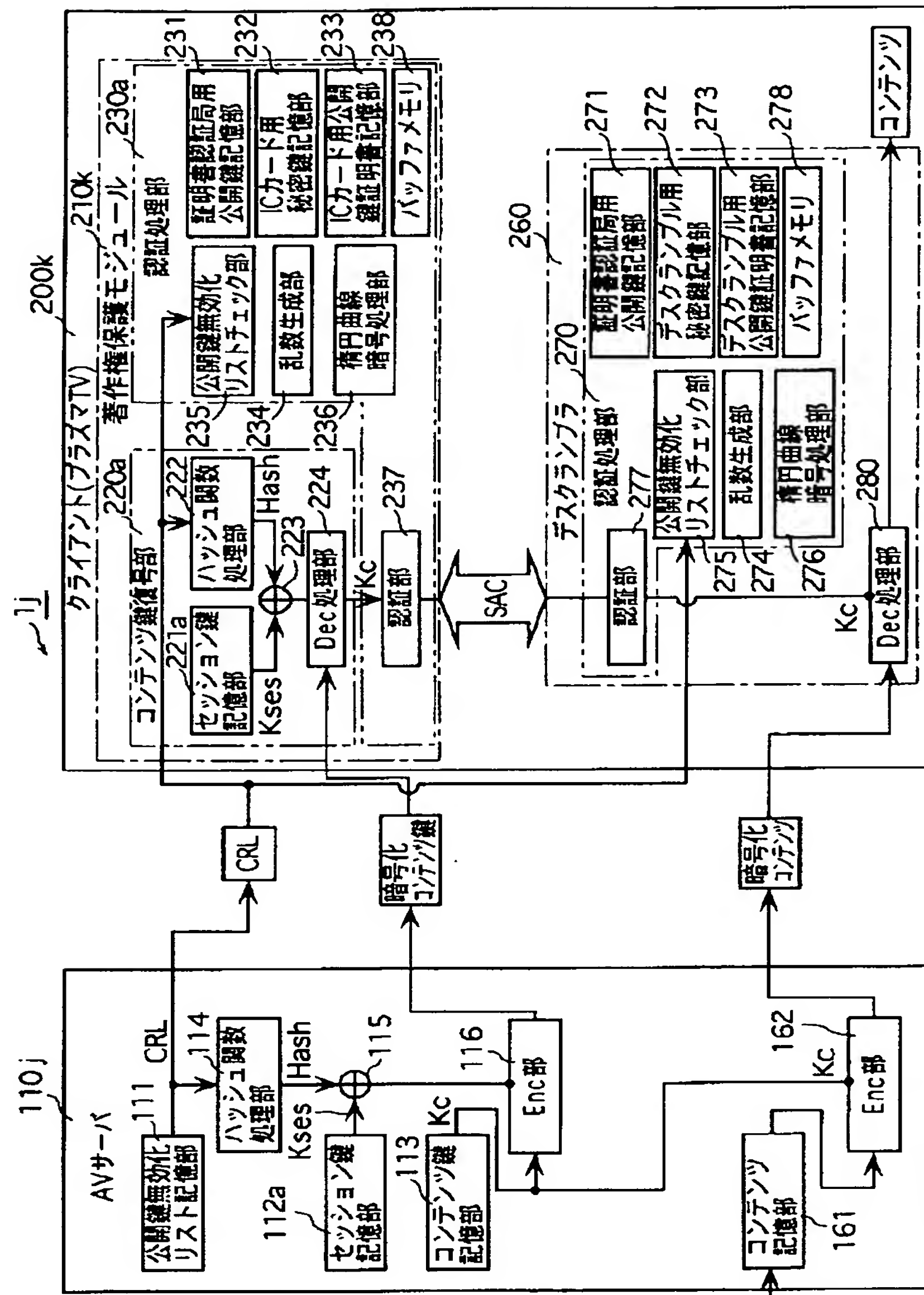


【図15】





【図18】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

ターマート (参考)

H 0 4 L 9/00

6 7 5 D

(72) 発明者 永井 隆弘

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 石原 秀志

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内



F ターム(参考) 5B017 AA03 BA07 CA09 CA16  
5J104 AA07 AA08 AA12 AA16 EA05  
EA18 JA01 JA03 JA21 JA31  
KA02 KA05 KA15 LA01 LA03  
LA06 NA02 NA35 NA37 NA38  
NA40 NA41 NA42



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☒ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**